Cybersecurity Updates Affecting Medtronic Implantable Cardiac Device Programmers: FDA Safety Communication

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities that may introduce risks for certain medical devices and hospital networks. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities is already publicly available.

A security firm has identified 11 vulnerabilities, named "URGENT/11." These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function.

These vulnerabilities exist in IPnet, a third-party software component that supports network communications between computers. Though the IPnet software may no longer be supported by the original software vendor, some manufacturers have a license that allows them to continue to use it without support. Therefore, the software may be incorporated into other software applications, equipment, and systems which may be used in a variety of medical and industrial devices that are still in use today.

Security researchers, medical device manufacturers, and the FDA are aware that some versions of the following operating systems are affected. Please note the vulnerable IPnet software component may not be included in all versions of these operating systems:

- VxWorks (by Wind River)
- Operating System Embedded (OSE) (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)
Some medical device manufacturers are already actively assessing which devices that use these operating systems are affected by URGENT/11 and identifying risk and remediation actions. Several manufacturers have also notified their customers consumers with devices determined to be affected so far, which include an imaging system, an infusion pump, and an anesthesia machine. The FDA expects that additional medical devices will be identified that contain one or more of the vulnerabilities associated with the original IPnet software.

Recommendations for Manufacturers

- Conduct a risk assessment, as described in FDA's cybersecurity postmarket guidance, to evaluate the impact of these vulnerabilities to your medical device portfolio and develop risk mitigation plans. Please keep in mind that the nature of the vulnerabilities allows the attack to occur undetected and without user interaction. Because an attack may be interpreted by the affected device as normal and benign network communications, it may remain invisible to existing security measures.

- Work with the operating system vendor to identify if a patch is available and implement recommended mitigation methods. Medical device manufacturers will need to evaluate and validate the patch for their devices.

- Ensure any mitigations you may currently employ (for example: firewalls, virtual private network (VPN)) are not impacted by URGENT/11.

- Develop a plan for updating your medical device to accommodate a version of an OS (or a communication protocol) that is not impacted by the URGENT/11 vulnerabilities.

- Work with health care providers and facilities to determine affected medical devices and discuss and develop ways to ensure that risks are reduced to acceptable levels.

- Communicate with your customers and the user community regarding your assessment and recommendations for risk mitigation strategies and any compensating controls, to allow customers to make informed decisions about device use. Provide an Information Sharing Analysis Organization (ISAO) with any customer communications upon notification of your customers.

- Report medical devices you've identified as vulnerable to URGENT/11 to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) at ICS-CERT@HQ.DHS.GOV, so that this information can be added to its evolving list of products.

Recommendations for Health Care Providers

- Advise patients who use medical devices that may be affected.
• Remind patients who use medical devices to seek medical help right away if they think operation or function of their medical device changed unexpectedly.

• Work with device manufacturers to determine which medical devices in your facilities or in use by your patients could be affected by these vulnerabilities and develop risk mitigation plans.

Recommendations for Health Care Facility Staff (including, IT Staff)

• Monitor your network traffic and logs for indications that an URGENT/11 exploit is taking place.

• Use firewalls, virtual private networks (VPN), or other technologies that minimize exposure to URGENT/11 exploitation.

Recommendations for Patients and Caregivers

• Talk to your health care provider to determine if your medical device may be affected. Please be aware that health care providers may not have access to this information at the time of issuance of this communication. Device manufacturers should be reaching out to their customers as more information becomes available.

• Seek medical help right away if you think operation or function of your medical device changed unexpectedly.

URGENT/11 Cybersecurity Vulnerabilities

On July 30, 2019, the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security released an advisory about cybersecurity vulnerabilities called URGENT/11.

Since publication of the advisory, the FDA became aware that these vulnerabilities may affect other operating systems that use the IPnet. Currently, VxWorks and IPnet are owned by Wind River. IPnet was originally manufactured by Interpeak. Before Wind River purchased IPnet, Interpeak licensed this software to other Real Time Operating System (RTOS) vendors to integrate into their operating systems. IPnet may also have been incorporated into other software applications, equipment, and systems.

For more information about URGENT/11 Cybersecurity Vulnerabilities see:

• [Department of Homeland Security Cybersecurity Infrastructure Security Advisory - October 1, 2019](#)

• [Department of Homeland Security Cybersecurity Infrastructure Security Advisory - July 29, 2019](#)
FDA Actions

The FDA is working closely with other federal agencies, manufacturers, and security researchers to identify, communicate and prevent adverse events related to the URGENT/11 vulnerabilities.

The FDA will continue to assess new information concerning the URGENT/11 vulnerabilities and will keep the public informed if significant new information becomes available.

Reporting Problems with Your Device

If you think you had a problem with your device or a device your patient uses, the FDA encourages you to report the problem through the MedWatch Voluntary Reporting Form.

Health care personnel employed by facilities that are subject to the FDA's user facility reporting requirements should follow the reporting procedures established by their facilities.

Questions?

If you have questions, email the Division of Industry and Consumer Education (DICE) at DICE@FDA.HHS.GOV or call 800.638.2041 or 301.796.7100.