MEDTECH INSIGHT
CITELINE COMMERCIAL

01 Oct 2019 | **News**

Cybersecurity Vulnerability Could Seriously Impact Wide Range Of Medtech Industry, FDA Warns

by Ferdous Al-Faruque

The US agency issued a safety communication on 1 October warning manufacturers, providers and patients of 11 serious exploits on a wide range of connected medical devices that could allow malicious hackers to not just steal patient data, but harm patients by altering how the devices function.

The US Food and Drug Administration is warning health-care providers and the medtech industry of serious vulnerabilities on certain operating systems used in medical devices that could allow malicious hackers to harm patients. While no one has reportedly been harmed yet, the agency says, some attacks could go undetected because of the way the vulnerabilities work.

On 1 October, the agency issued a safety communication about security vulnerabilities found in a number of operating systems that affect a wide range of products in the automotive, aeronautics, consumer and health-care industries. Back in July, security researchers found the 11 vulnerabilities, now called "URGENT/11," that could allow malicious hackers to take over a device and steal patient data.

The FDA says it was made aware of the vulnerability when a security researcher wrote about it in *Wired magazine* and published it on their personal website. "URGENT/11 affects several operating systems that may then impact certain medical devices connected to a communications network, such as wi-fi and public or home internet, as well as other connected equipment such as routers, connected phones and other critical infrastructure equipment," the FDA wrote. "These cybersecurity vulnerabilities may allow a remote user to take control of a medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent a device from functioning properly or at all."

© Citeline 2024. All rights reserved.

Medtech companies have already begun reaching out to patients and providers to update them on the vulnerabilities and what to do about them. While not naming any company in particular, the FDA says the vulnerabilities affect a range of devices, including an imaging system, an infusion pump and an anesthesia machine.

> *"Medical device manufacturers are actively assessing which devices may be affected by these vulnerabilities, and identifying risk and remediation actions." – Alison Hunt*

The issue seems to be due to an internet protocol software that allows devices to communicate over networks called IPnet.

“Due to the complexities in how the code from the IPnet third-party software component was incorporated into various medical devices and the availability of the exact operating system versions impacted, it will be difficult to develop a comprehensive list” of affected devices, FDA spokesperson Alison Hunt said. “Additionally, IPnet may have been incorporated into other software applications, equipment and systems.

“Medical device manufacturers are actively assessing which devices may be affected by these vulnerabilities, and identifying risk and remediation actions,” she added. “Manufacturers have been asked to evaluate the impact of these vulnerabilities on their devices, and to communicate their findings and recommendations for risk reduction to their customers, as they have the most knowledge regarding their products.”

The FDA will continue to update the list of devices affected by the vulnerability at *here*.

The third-party software is part of a number of real-time operating systems (RTOP) that are used in medical devices and health-care systems. The following is a list provided by the FDA of RTOPs that are affected:

- VxWorks manufactured by Wind River;
- Operating System Embedded (OSE) manufactured by ENEA;
- INTEGRITY manufactured by GreenHills;

© Citeline 2024. All rights reserved.

- ThreadX manufactured by Microsoft;
- ITRON manufactured by TRON;
- and ZebOS manufactured by IP Infusion.

There have not been any reports of adverse events yet where a malicious hacker harmed a patient by exploiting the vulnerabilities, the agency says. However, the regulators warn that the nature of the vulnerabilities mean an attack could "...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."

Amy Abernethy, the FDA's principal deputy commissioner, urged device-makers to stay vigilant for potential exploits of the vulnerabilities and be proactive about trying to address them.

For now the FDA is asking manufacturers to work with providers to figure out which devices are affected and develop mitigation plans. The agency is also urging patients to talk to their physicians to get more information on whether their device is vulnerable and what action they should take.

> *"The risk of patient harm if such a vulnerability were left unaddressed could be significant." – Suzanne Schwartz*

In general, the FDA says device-makers should refer to the agency's *cybersecurity postmarket guidance* to determine the impact and discover potential solutions to the URGENT/11 vulnerabilities. (Also see "*'Sharing' Organizations Stay In Final Post-Market Cybersecurity Guidance*" - Medtech Insight, 29 Dec, 2016.)

"Medical device manufacturers should work with operating system vendors to identify available patches and other recommended mitigation methods, work with health-care providers to determine any medical devices that could potentially be affected, and discuss ways to reduce associated risks," the agency wrote.

"While we are not aware of patients who may have been harmed by this particular cybersecurity vulnerability, the risk of patient harm if such a vulnerability were left unaddressed could be significant," cautioned Suzanne Schwartz, deputy director of the Office of Strategic Partnerships

© Citeline 2024. All rights reserved.

and Technology Innovation within the FDA's Center for Devices and Radiological Health. "It's important for manufacturers to be aware that the nature of these vulnerabilities allows the attack to occur undetected and without user interaction. Because an attack may be interpreted by the device as a normal network communication, it may remain invisible to security measures."

© Citeline 2024. All rights reserved.