PUBLICATION

FDA Issues Cybersecurity Alert to Health Care Providers and Device Manufacturers

Authors: Samuel Lanier Felker
October 03, 2019

The U.S. Food and Drug Administration took the unprecedented step this week of issuing an alert to health care providers and device manufacturers about potentially serious security flaws that may allow hackers to remotely take control of medical devices or otherwise interrupt patient care. While stating that it is currently unaware of any confirmed adverse events related to these cybersecurity vulnerabilities, the FDA stated that software to exploit these vulnerabilities is publicly available. This raises the risk profile for health care providers, manufacturers, and patients using a variety of medical devices with cyber capabilities.

The specific cyber vulnerabilities, which the FDA dubbed URGENT/11, exist in a commonly used third-party software component that supports network communications between computers and is commonly used in some medical devices. Prior to this alert, the FDA, through their Fact Sheet and other communications, warned that medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. However, the FDA relied primarily on device manufacturers to mitigate the risk through product design and cybersecurity updates.

In this alert, the FDA identified IPnet as the culprit. IPnet is a third-party software component which may be incorporated into applications, equipment, and systems that are used in a variety of medical devices. This software may no longer be supported by the original vendor, yet some device manufacturers have a license that allows them to continue to use IPnet despite the lack of vendor support. The following operating systems have already been identified by the FDA as having the potential for vulnerability:

- 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)

We agree with the FDA's recommendations that health care providers conduct risk assessments to search for potential URGENT/11 vulnerabilities in their networks and that they develop risk mitigation plans. Health care providers should ensure that medical device software is regularly updated and that all available security patches have been installed. Additionally, providers should instruct IT Staff to monitor network traffic and logs for indications that an URGENT/11 exploit is taking place. To minimize exposure to exploitation of the vulnerabilities, we also recommend the use of firewalls and VPNs.

Due to the potential for numerous legal risks, we recommend that counsel work with providers and IT staff to implement both compliance plans and incident response plans to ensure preparedness for any exploitation of the URGENT/11 vulnerabilities. Additionally, counsel should assist in addressing any vulnerabilities that are discovered and should work with IT staff to assess potential solutions, in consultation with device manufacturers, and ensure that steps are taken to provide adequate network protection.

If you have any questions regarding these issues or any other cybersecurity or data privacy-related matters, please contact Sam Felker or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.