The Patch Act: Now What?

How medical device manufacturers can take proactive action.

Troy Ament, Fortinet Healthcare CISO

Thanks to an inclusion in the omnibus spending package passed by Congress in December, the FDA has new authority to establish medical device security requirements for manufacturers. The Protecting and Transforming Cyber Healthcare (Patch) Act has been praised by healthcare organizations.

The ability of cyber-attackers to access a healthcare provider's network environment through security gaps or vulnerabilities is increasing. And regrettably, Internet of Medical Things (IoMTs) and other devices may be severely affected when bad actors can travel laterally through a network—and have a a direct negative impact on patient care and safety.

The FDA's new authority has major implications for medical device manufacturers, though there's still a lot to be revealed. There are some steps that can be taken proactively now to prepare even as the FDA works through the public regulatory process to produce more detailed requirements and guidance. What can be anticipated is that failure to comply with these mandates will impact device certification by the FDA. Waiting to formulate a plan for working with these new regulations is going to leave an organization behind and scrambling to keep up. It's time to get those ducks in a row.

Greater Transparency

One thing we expect as new guidelines are brought to fruition is that the FDA will require medical device manufacturers to be more transparent about the technologies they're selling—in a way they've never had to be. One thing that manufacturers may need to provide moving forward is a software bill of materials: an inventory of all the hardware and software that is contained in their technologies.

This could include things like Java, Log4j, Microsoft operating systems, other Linux operating systems contained in their technologies—all things they've never had to disclose before. And these are the types of systems and software often associated with vulnerabilities.

Navigating New Cybersecurity Guidelines

Until recently, the FDA's medical device approval process didn't require cybersecurity controls. The next steps by the FDA will determine the breadth of how cybersecurity will need to be embedded in medical devices if they're to be approved by the agency.

Manufacturers should be closely following these upcoming FDA guidelines on cybersecurity. However, even as the agency goes through the public regulatory process, there are some key areas we should expect them to focus on—and for which manufacturers can prepare, including what's known as the cybersecurity lifecycle of a device.

What does this mean exactly? Well, these devices previously, by nature, were built to not change after they were approved by the FDA. But now, going forward, those devices may need the ability to be patched. Let's say that within the software bill of materials, a device runs a certain operating system, and that operating system has a vulnerability. Manufacturers will likely be required to have a mechanism to update those devices post-market and fix those vulnerabilities. That's where all that disclosure around things like what software is contained within a device will come into play. Companies may need to show they have a plan to address things like a Log4j vulnerability—which, as we've seen historically, is a very real possibility.

Establishing Stricter Governance

To meet the requirements of the Patch Act and forthcoming FDA requirements, one of the first things most organizations should do, depending on their cybersecurity maturity level, is look at stricter governance to assess the risk of the new devices they're to be building and seeking the FDA's approval for.

Medical device manufacturers should implement technologies that prevent and protect devices from vulnerabilities and exploits. Those technologies vary; medical device manufacturers will be evaluating network security applications like firewalls, implementing models like zero trust, adding endpoint technology to detect and respond to threats, and so on.

Zero trust and next-generation firewalls are a good place to start—and we're already starting to see some companies building these into their devices. There may also be the need to add capabilities for orchestration and the automation of patches to those devices to remediate vulnerabilities. Imagine that an organization has 50,000 pieces of lab equipment across the globe. It won't be possible to remediate all these manually in a timely fashion; the ability to automate this will be key.

For many organizations, this will also be a time to establish a more formalized strategy and set of controls for assessing the cybersecurity risk within new devices. They are going to need to operationalize all of this. They should do strategic planning to engineer governance and cybersecurity lifecycle into every device and, more importantly, into their development teams. Security will need to be embedded into the development and design of devices from the get-go; bolting it on after the fact won't suffice.

Supply Chain Attacks

Now that medical device manufactures will require a cybersecurity lifecycle that includes patching of new vulnerabilities, this will increase the attack surface. That's because devices will be changed more frequently post-maket. Adversaries may look to compromise software development cycles and inject vulnerabilities that allow bad actors to compromise IoMT devices, healthcare system networks, and potentially cause patient safety issues.

The Road Ahead

The upcoming effort by the FDA is important and long-awaited step in securing IoMT devices for greater patient safety. The onus may now be on medical device manufacturers to do all they can to ensure that safety, so new strategy and processes are a must. Getting a strong plan in place now to ensure compliance will be key to not only protecting patients, but also ensuring a company will continue to be able to bring new devices to the market with FDA approval.

Originally published by CSO in May 8, 2023.

July 19, 2023 11:35 AM

2153400-0-0-EN