BIOTRONIK Statement on the Cybersecurity Updates Affecting Medtronic Implantable Cardiac Device Programmers

October 18, 2018

On October 11, the US Food and Drug Administration (FDA) issued a Safety Communication regarding cybersecurity updates affecting Medtronic implantable cardiac device programmers, based on an NCCIC Advisory.[1] According to the FDA's communication, Medtronic is issuing a software update to address a safety risk caused by cybersecurity vulnerabilities associated with the internet connection in two models of programmers used to download software from the manufacturer's software distribution network (SDN). Successful exploitation of these vulnerabilities would allow an adversary to influence this communication and respond with malicious updates to the programmer software that could change a programmer's functionality or a connected implantable device.[2]

The FDA's Safety Communication refers to several vulnerabilities in Medtronic's implantable cardiac device programmers. None of BIOTRONIK's devices, programmers or networks are affected by these cybersecurity vulnerabilities or the corrective measures that have been subsequently taken. Neither are any corrective measures necessary for BIOTRONIK's devices.

BIOTRONIK Renamic programmers use certificate-based mutual authentication to establish a VPN tunnel. Prior to downloading new programmer software, the Renamic device verifies that it is still connected to the authenticated server.

The Renamic programmer recognizes and rejects illegitimate software update files. The files used to update BIOTRONIK Renamic programmers use a digital signature to ensure authenticity and integrity of the software update. These update files are transferred via a secure HTTPS connection to the programmer device. Moreover, BIOTRONIK's remote programmer software update system is not based on commercial off-the-shelf software with known vulnerabilities. Together, these design elements strengthen the programmer against vulnerabilities that allow unauthorized changes in programmer functionality.

Safety is paramount to the design and production of all BIOTRONIK devices and is at the center of everything we do. As part of its established cybersecurity processes, BIOTRONIK continuously analyzes external reports and assesses device security. BIOTRONIK takes these additional steps to ensure the safety and efficacy of all of its systems.

---

[1] Advisory ICSMA-18-058-01, Medtronic 2090 Carelink Programmer Vulnerabilities (Update B), Original release date: February 27, 2018 | Last revised: October 11, 2018, https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-01

[2] U.S. Food & Drug Administration, Cybersecurity Updates Affecting Medtronic Implantable Cardiac Device Programmers: FDA Safety Communication, October 11, 2018, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm?utm_campaign=Cybersecurity%20Updates%20-%20Medtronic&ut%E2%80%A6