BIOTRONIK Statement on the Publication 'Security Testing of the Pacemaker Ecosystem'

August 12, 2019

The work 'Security Testing of the Pacemaker Ecosystem' was recently published as a master's thesis, authored by Mr. Anders Been Wilhelmsen and Mr. Eivind Skjelmo Kristiansen. This publication investigates the state of cybersecurity of BIOTRONIK's ICS 3000 – a programmer for BIOTRONIK implantable cardiac pacemakers, defibrillators and monitors that is used by healthcare professionals during the implantation procedure and follow-ups.

ICS 3000 programmers were distributed between 2001 and 2012. In the publication, the authors report about several cybersecurity weaknesses such as:

- Vulnerabilities in third party software components
- Lack of login-in functionality after startup

The central thesis of this publication is based on programmer software and not the programmer hardware. The authors inspected the programmer software PSW 1004.U which was released in February 2011.

Since the publication inspects outdated, eight-year-old software, cybersecurity measures implemented after 2011 are not considered.

While some of the vulnerabilities reported in the publication previously existed, software updates in the past years have already addressed these to make the programmer resilient against potential adversarial attacks. The programmer's software architecture has been carefully designed in a way that vulnerabilities existing in third party software cannot be exploited due to the lack of affected interfaces, features, and driver software (e.g. no TCP/IP interface, limited USB drivers, and no open PDF/XML/JPG features). Current programmer software releases provide an authentication mechanism through individual passwords to allow restriction of device access.

BIOTRONIK maintains a rigorous cybersecurity management process that is carefully designed according to the recommendations of the FDA's cybersecurity guidance to identify and control cybersecurity risks in all its products and systems. As part of this, BIOTRONIK continuously analyzes external reports, assesses device security and updates its devices accordingly.

BIOTRONIK remains strongly committed to a high standard of resilience against cyberattacks while developing innovations that save and improve the lives of millions diagnosed with heart and blood vessel diseases.

Should you need further information, please contact us:

For Healthcare Professionals: product.support@biotronik.com

For Patients: patients@biotronik.com

For Press: press@biotronik.com