ICSMA-22-067-01 Axeda Alert for Model 3300 LATITUDE™ Programming System

As part of a coordinated vulnerability disclosure between CyberMDX and Boston Scientific, an Industrial Control Systems Advisory (ICSA) has been published for Axeda software used on the Model 3300 LATITUDE™ Programming System. The advisory has been published at: ICS Advisory (ICSA-22-067-01) PTC Axeda agent and Axeda Desktop Server | CISA.[1] Boston Scientific is not named as an affected manufacturer because of the configuration and security measures on the Model 3300 LATITUDE Programming System.[1]

Summary:

- The Model 3300 LATITUDE Programming System (Programmer) interrogates and programs Boston Scientific Cardiac Implantable Electronic Devices (CIEDs)[2] using a wanded handshake to establish wireless telemetry by trained health care professionals.
- Axeda software is used by the Programmer to install new software applications when commanded by the user.
- Based on the existing security measures of the Programmer and the configuration of Axeda, exploitation of these vulnerabilities can only occur if an attacker physically accesses a Programmer.
- CyberMDX has published a list of affected manufacturers. Due to the limited impact to the Programmer, Boston Scientific was not named in this alert.
- There have been no reported or confirmed breaches associated with Axeda software on the Model 3300 LATITUDE Programming System.
- There are no actions aside from maintaining physical security of the Programmer and removing PHI[3] before retiring or removing a Programmer from your facility.
- Boston Scientific has initiated a previously planned replacement of Axeda.
- Axeda is not used by any other Boston Scientific system.

Vulnerability Detail:

CyberMDX performed a security investigation of Axeda software and discovered vulnerabilities. Based on the Axeda configuration of the Programmer, only the following are used in the Model 3300 LATITUDE Programming System:

- XGate software, vulnerability reference: CVE-2022-25249, CWE-22, CVSS v3.1 score 7.5
- xBase39 library, vulnerability reference: CVE-2022-25252, CWE-703, CVSS v3.1 score 7.5

The Axeda software xGate and xBase39 library are only run when the user prompts the Programmer to check for software updates and when the user has initiated the software update process. Therefore, xGate and xBase329 are run exclusively when performing Programmer software installations and not for interrogation or Programming a CIED. There are no remote login capabilities. All software running on the Programmer is authorized through a cryptographic signature verification at run time. After xGate and XBase39 run, the Programmer reboots into an install mode that authorizes changes through a cryptographic signature verification. All network connections are encrypted and restricted to outbound traffic only to known Boston Scientific and affiliate addresses.

Please contact Boston Scientific Technical Services with any questions about this bulletin, precautionary measures, or any other concerns regarding the Model 3300 LATITUDE Programming System security.

Revision 1 – March 8, 2022

[1] https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01 and https://www.cybermdx.com/access7-affected-devices/

[2] Including implantable pacemakers and defibrillators

[3] Instructions for removing protected health information (PHI) from a programmer are outlined in the user's manual

United States Technical Services
1.800.CARDIAC (227.3422)
tech.services@bsci.com

International Technical Services
+32 2 416 7222
intltechservice@bsci.com

Asia Pacific Technical Services
+61 2 8063 8299
aptechservice@bsci.com