ANZCDACC Advisory Notice 18th of January 2019

Device: Medtronic Carelink 2090 and the Carelink Encore 29901/29901A programmers (All serial numbers)

TGA Reference: RC-2018-RN-01351-1

Advisory grade TGA: TBA

ANZDACC Advisory Grade: Routine

Description:

Currently, the Medtronic CareLink™ 2090 and CareLink Encore™ 29901 programmers receive new software from one of two routes: using the USB port, or using a network connection via the Software Distribution Network (SDN). The SDN is a worldwide network that allows the download of new or updated software to above mentioned programmers via the internet.

Vulnerabilities have been identified in the SDN download process that may allow an individual with malicious intent to update the programmers with non-Medtronic software during an SDN download. To date, Medtronic has received zero (0) reports to indicate that such an issue has occurred. Medtronic issued an initial security bulletin in February 2018 with an update in June 2018 which can be found at www.medtronic.com/security. However, further review of these vulnerabilities with the U.S. Food & Drug Administration (FDA) and external researchers led to the conclusion that the process for updating software through the SDN may introduce risks that, if not fully mitigated, could result in harm to a patient depending on the extent and intent of a malicious cyberattack and the patient's underlying condition. To date, neither such an attack nor resultant patient harm has been observed.

Beginning 11 October 2018, Medtronic will be disabling the SDN for programmer updates and will rely solely on the USB update method.

Number of CIEDs affected in Australia and New Zealand:

Zero (0)

Presentation:

If you select the "Install from Medtronic" button, it will not result in software installation because access to the external SDN is no longer available.

Advice:

- Continue to use the programmers for programming, testing and evaluation of CIED patients. Network connectivity is not required for normal CIED programming and similar operation.
    - Other Medtronic-provided features that require network connections are not impacted by these vulnerabilities (e.g. SessionSync™). You may continue to use such features.
- Do not attempt to update the programmer via the SDN. If you select the "Install from Medtronic" button, it will not result in software installation because access to the external SDN is no longer available.
    - Future programmer software updates must be received directly from a Medtronic representative.

- Medtronic recommends customers operate the programmers within well managed IT networks. Consult with your IT department regarding the security of your network. For recommended actions to better secure your computer network environment, refer to https://www.nist.gov/cyberframework or other cybersecurity guidance.
- Reprogramming or updating of cardiovascular implantable electronic devices (CIED) is **not required** as a result of this correction and prophylactic CIED replacement is **not recommended** and should not be performed.

Further Medtronic Actions:
Medtronic is working to implement security updates for the programmers that will further address these vulnerabilities and will be implemented pending regulatory agency approvals. We will inform you as they become available.

The ANZCDACC encourage you to report any adverse event or near (potential) adverse event associated with the use of a medical device including any abnormal CIED or lead function. We encourage reporting to ANZCDACC directly via the Committee chair Dr Paul Gould drpgould@gmail.com and to the following regulators.

In Australia, report to the TGA;

Online   https://www.tga.gov.au/reporting-problems

In New Zealand, report to Medsafe;

Post   Compliance Management Branch, Medsafe, PO Box 5013, Wellington 6145.

Email   devices@moh.govt.nz

Fax   04 819 6806