Radiofrequency remote monitor software patch update without cybersecurity implantable cardioverter-defibrillator firmware update increases the risk of inappropriate implantable cardioverter-defibrillator therapies

Xiaoxiao Qian, MD,* Courtney J. Channels, NP,† Stephen A. Gaeta, MD, PhD, FHRS,† Marc H. Wish, MD, FHRS,† Brewer Matthews, BS,‡ Brett D. Atwater, MD, FHRS,† Vineet Kumar, MD, FHRS†

*From the *Division of Cardiology, Inova Heart and Vascular Institute, Falls Church, Virginia, †Division of Cardiac Electrophysiology, Inova Heart and Vascular Institute, Falls Church, Virginia, and ‡Abbott Laboratories, Washington, DC.*

Introduction

In August 2016 Muddy Waters LLC released a report claiming that certain St. Jude Medical/Abbott cardiovascular implantable electronic devices (CIEDs) were vulnerable to cyberattack through the Merlin@home™ radiofrequency (RF) remote monitoring system. In January 2017 the United States Food and Drug Administration (FDA) released a statement providing information and making recommendations to reduce the risk of patient harm due to cybersecurity vulnerabilities. The FDA confirmed that an altered Merlin@home RF communicator could be used to modify programming commands to the CIEDs, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks. In response, on January 9, 2017, St. Jude Medical/Abbott issued a software patch for the Merlin@home RF communicator to reduce cyberattack vulnerabilities. It is believed that this patch was successfully programmed in nearly 100% of actively used Merlin@home RF communicators. On August 29, 2017, St. Jude Medical/Abbott released CIED firmware updates to reduce cybersecurity vulnerabilities among their RF-enabled pacemakers, including cardiac resynchronization therapy pacemakers and on April 17, 2018, St. Jude Medical/Abbott released firmware updates to strengthen cybersecurity performance in their line of RF-enabled implantable cardioverter-defibrillators (ICD) and cardiac resynchronization therapy defibrillators. Updating the CIED firmware requires an in-person manual device interrogation, takes approximately 3 minutes to complete, and is associated with a low risk of firmware update–related complications,[1–3] including palpitations, pocket stimulation, general discomfort, and failure to complete the update with the device remaining in backup mode. On November 22, 2019, St. Jude Medical/Abbott released a clinical update that showed that approximately 25% of all patients with CIEDs followed on Merlin@home had received the firmware updates and that the frequency of firmware update–related complications was 0.032%.[1] In 2020 Saxon and colleagues[4] published updated frequency and safety data regarding St. Jude Medical/Abbott cybersecurity firmware updates. They found that overall only 24% of active CIEDs had updated firmware and that globally a

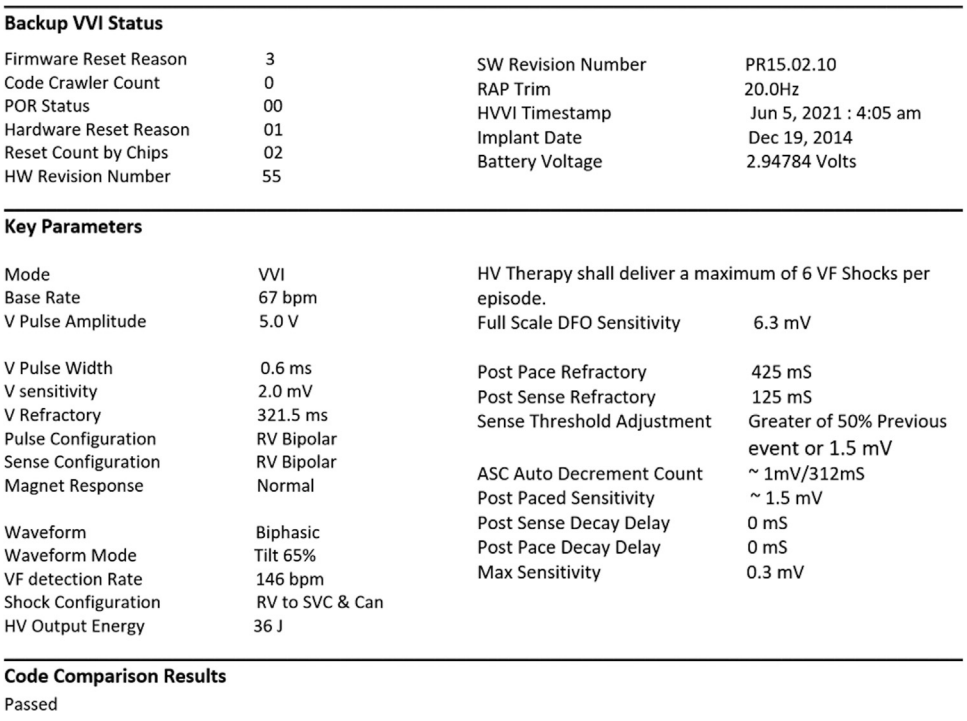
KEY TEACHING POINTS

- St. Jude Medical/Abbott Medical implantable cardioverter-defibrillators with outdated firmware can reset into hardware mode owing to event queue overload and this increases the risk of inappropriate therapies.
- Updated firmware of St Jude Medical/Abbott Medical implantable cardioverter-defibrillators can prevent inappropriate therapies owing to event queue overload.
- All patients with eligible St. Jude Medical/Abbott Medical devices should have firmware updated.

KEYWORDS Cardiovascular implantable electronic devices; Firmware; Defibrillation; Atrial fibrillation; Cybersecurity
(Heart Rhythm Case Reports 2022;8:69–72)

Funding Sources: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. Disclosures: All authors have no conflict of interest to disclose. **Address reprint requests and correspondence:** Dr Vineet Kumar, Division of Cardiac Electrophysiology, Inova Heart and Vascular Institute, 3300 Gallows Rd, Falls Church, VA 22042. E-mail address: Vineet.Kumar@inova.org.

https://doi.org/10.1016/j.hrcr.2021.12.016



Backup VVI Status

Firmware Reset Reason	3	SW Revision Number	PR15.02.10
Code Crawler Count	0	RAP Trim	20.0Hz
POR Status	00	HVVI Timestamp	Jun 5, 2021 : 4:05 am
Hardware Reset Reason	01	Implant Date	Dec 19, 2014
Reset Count by Chips	02	Battery Voltage	2.94784 Volts
HW Revision Number	55		

Key Parameters

Mode	VVI	HV Therapy shall deliver a maximum of 6 VF Shocks per episode.	
Base Rate	67 bpm		
V Pulse Amplitude	5.0 V	Full Scale DFO Sensitivity	6.3 mV
V Pulse Width	0.6 ms	Post Pace Refractory	425 mS
V sensitivity	2.0 mV	Post Sense Refractory	125 mS
V Refractory	321.5 ms	Sense Threshold Adjustment	Greater of 50% Previous event or 1.5 mV
Pulse Configuration	RV Bipolar		
Sense Configuration	RV Bipolar	ASC Auto Decrement Count	~ 1mV/312mS
Magnet Response	Normal	Post Paced Sensitivity	~ 1.5 mV
Waveform	Biphasic	Post Sense Decay Delay	0 mS
Waveform Mode	Tilt 65%	Post Pace Decay Delay	0 mS
VF detection Rate	146 bpm	Max Sensitivity	0.3 mV
Shock Configuration	RV to SVC & Can		
HV Output Energy	36 J		

Code Comparison Results

Passed

Figure 1 Device interrogation in the emergency department showed that the patient's defibrillator was in VVI backup mode with base rate at 67 beats per minute and ventricular fibrillation detection rate at 146 beats per minute.

total of 9 pacemakers (9/220,500) and 8 ICDs (8/196,800) required replacement as a result of irreversible reversion to backup mode with loss of defibrillation or pacing programmability as a result of the firmware update procedure. They found that pacemaker dependency was independently associated with a lower likelihood of firmware update, which the authors concluded was "justifiable in light of the small number of devices that required replacement due to non-programmability and backup mode pacing." Further, the authors concluded that "deferring an update is a justifiable decision as there have been no reported cybersecurity breaches impacting the devices included in any of the FDA advisories to date."

We present a case of a patient with a St. Jude Medical/Abbott Fortify Assura^{TM} ICD without cybersecurity firmware update who received multiple inappropriate ICD shocks likely in the setting of atrial fibrillation (AF) with rapid ventricular response after the Merlin@home RF communicator software patch resulted in reversion to hardware/backup mode. This case identifies a second important reason to consider updating St. Jude Medical/Abbott CIED cybersecurity firmware.

Case report

The patient is a 56-year-old woman with a history of sudden cardiac arrest in 2002 status post implantation of a secondary prevention St. Jude Medical/Abbott dual-chamber ICD, paroxysmal AF, and mitral valve repair in 2004 for severe mitral regurgitation who presented to the emergency department (ED) after receiving multiple shocks from her ICD. She reported sitting on her couch without antecedent chest pain, shortness of breath, palpitations, lightheadedness, or dizziness prior to the shock. A witness reported that her body suddenly jolted and rose up slightly from the couch and the patient reported that it was acutely painful. After the shock she felt well but 2 hours later, she received a second shock, felt vibration from her CIED site, and activated EMS. Upon arrival to the ED, she was asymptomatic and her vitals and physical examination were normal. Laboratory work revealed normal electrolytes and negative troponins. Twelve-lead electrocardiogram showed sinus rhythm and ventricular pacing at 67 beats per minute (BPM). ICD interrogation indicated that the device was in hardware/backup mode (Figure 1): bradycardia pacing was set to VVI 67 BPM and ventricular tachycardia/ventricular fibrillation (VT/VF) detection was a single zone at 146 BPM with 12 intervals to detection. There was no electrogram (EGM) recorded during the shocks because no EGMs were stored in hardware/backup mode. Review of her device interrogation 1 month prior to the episode confirmed that her final programmed settings were DDI 50 BPM with VT detection at 160 BPM and VF detection at 214 BPM.

Further investigation revealed that the patient's CIED generator was last exchanged in 2014 and despite enrolling in Merlin@home remote monitoring and having frequent in-person device checks the cybersecurity firmware upgrade had not been completed. The ICD generator interrogation revealed error code 3, confirming that the ICD entered hardware/backup mode owing to event queue overload (EQO) after it had several RF connection/disconnection events with the Merlin@home system over a short period of time.

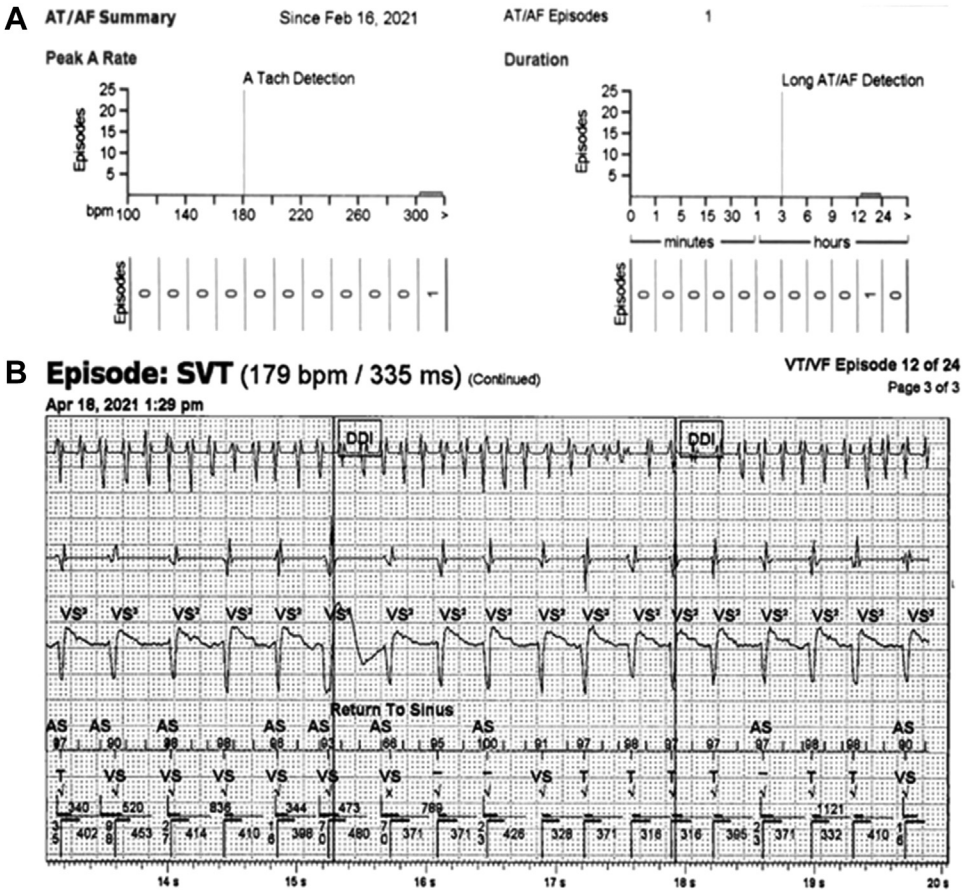


Figure 2 Device interrogation 4 weeks prior to event showed the following: **A:** 1 episode of atrial fibrillation (AF) with atrial rate >300 beats per minute, which lasted for about 14 hours; **B:** same episode of AF with ventricular rate >179 beats per minute.

In the setting of older version firmware pr15.02.10, this frequent connection/disconnection behavior indicates a potential cyberattack and the device is programmed to enter hardware/backup mode to avoid cyberattack vulnerabilities. Because the patient had not had recurrent ventricular tachyarrhythmia since the original ICD implantation in 2002 and her device interrogation 1 month prior to the event showed 1 episode of AF with sustained ventricular rates >150 BPM that lasted for 14 hours (Figure 2), the most likely explanation for her ICD shocks was inappropriate detection and treatment for AF with ventricular rates >146 BPM. Her ICD was reprogrammed to her original settings, she was prescribed rate-controlling medical therapy for her rapidly conducted AF, the cybersecurity firmware was upgraded to version pr15.02.1A, and she was discharged from the ED.

Discussion

Cyberattack of CIEDs could affect patients' confidentiality, interrupt remote monitoring, and even harm patients by changing the device settings or promoting early battery depletion; however, to date no known harm has occurred as a result of a CIED cyberattack.

The FDA currently allows for manufacturer-directed automatic remote programing of remote monitoring transmitters, including the Merlin@home RF communicator; our case illustrates that this process may inadvertently lead to patient harm. In our case the Merlin@home RF communicator software patch increased the risk of inappropriate ICD therapies owing to frequent RF connection/disconnection–related EQO events in the setting of outdated ICD firmware. EQO is a known phenomenon when CIEDs detect frequent connection/disconnection to the Merlin@home system. The worldwide frequency of CIEDs resetting to hardware/backup mode in response to the Merlin@home RF communicator among ~83,000 Ellipse, Fortify Assura, and Quadra Assura ICDs followed in the Merlin@home system was 0.30%.[5] As of June 20, 2020, the cumulative incidence rate based on worldwide sales of the aforementioned ICDs is 0.19%.[5] Of note, all EQO events have occurred in devices that had not undergone the cybersecurity firmware update. In our case it was impossible to confirm the underlying rhythm when she experienced ICD shocks because hardware/backup mode disabled EGM recordings, preventing the care team from tailoring device programming and medical therapies to her specific arrhythmia. Being in the hardware/backup mode increased the risk of inappropriate shocks in the setting of atrial tachycardia with ventricular rate above the VT/VF detection threshold, and this is most likely the cause of

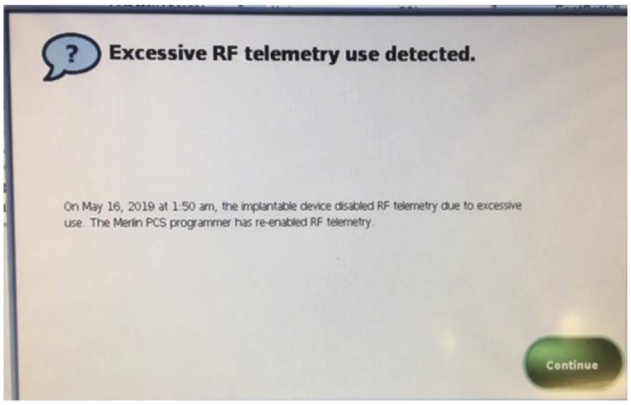


Figure 3 Sample error message when cardiovascular implantable electronic devices with updated firmware have frequent connection and disconnection to the Merlin@home system. RF = radiofrequency.

ICD shocks in our patient. In the updated version of firmware, the threshold for number of connections/disconnections and the duration to suspect RF attack was changed, and the response to possible RF attack is to disable the RF telemetry until the device is interrogated in person (Figure 3). No EQO events have been reported so far with the updated firmware.

This case highlights a second important reason to consider updating St. Jude Medical/Abbott CIED firmware: in addition to reducing the risk of cyberattack, firmware updates may minimize the risk of inappropriate ICD shocks among the 0.19%–0.3% of patients who experience EQO events from the Merlin@home RF communicator software patch. Incorporating this possibility into the patient discussion about the risks and benefits of firmware update would better assist shared decision-making. In response to this case and to comply with the FDA/St. Jude Medical/Abbott recommendations to update firmware of all eligible CIEDs, we requested all patients followed in the Inova Arrhythmia clinic with St. Jude Medical/Abbott CIEDs who had no previous firmware update to come to clinic for in-person firmware reprogramming. To date, a total of 61 patients complied with the request and 0 patients experienced an adverse reaction to firmware update.

Conclusion

This case of inappropriate ICD shocks demonstrates additional benefits of upgrading firmware in St. Jude Medical/Abbott CIEDs beyond cybersecurity threat.

References

1. Abbott. Clinical update. https://www.cardiovascular.abbott/content/dam/bss/divisionalsites/cv/pdf/reports/cyber_clinical_update_nov2019.pdf.
2. Baranchuk A, Alexander B, Campbell D, et al. Pacemaker cybersecurity: local experience with a firmware upgrade. Circulation 2018;138:1272–1273.
3. Alexander B, Neira V, Campbell D, et al. Implantable cardioverter-defibrillator-cybersecurity. Circ Arrhythm Electrophysiol 2020;13:277–279.
4. Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Rates of adoption and outcomes after firmware updates for Food and Drug Administration cybersecurity safety advisories. Circ Arrhythm Electrophysiol 2020;13:869–872.
5. Abbott. Product Performance Report. 2020. Second edition. https://www.cardiovascular.abbott/content/dam/bss/divisionalsites/cv/hcp/products/product-performance-reports/documents/Abbott-Product-Performance-Report-2020-Second-edition.pdf.