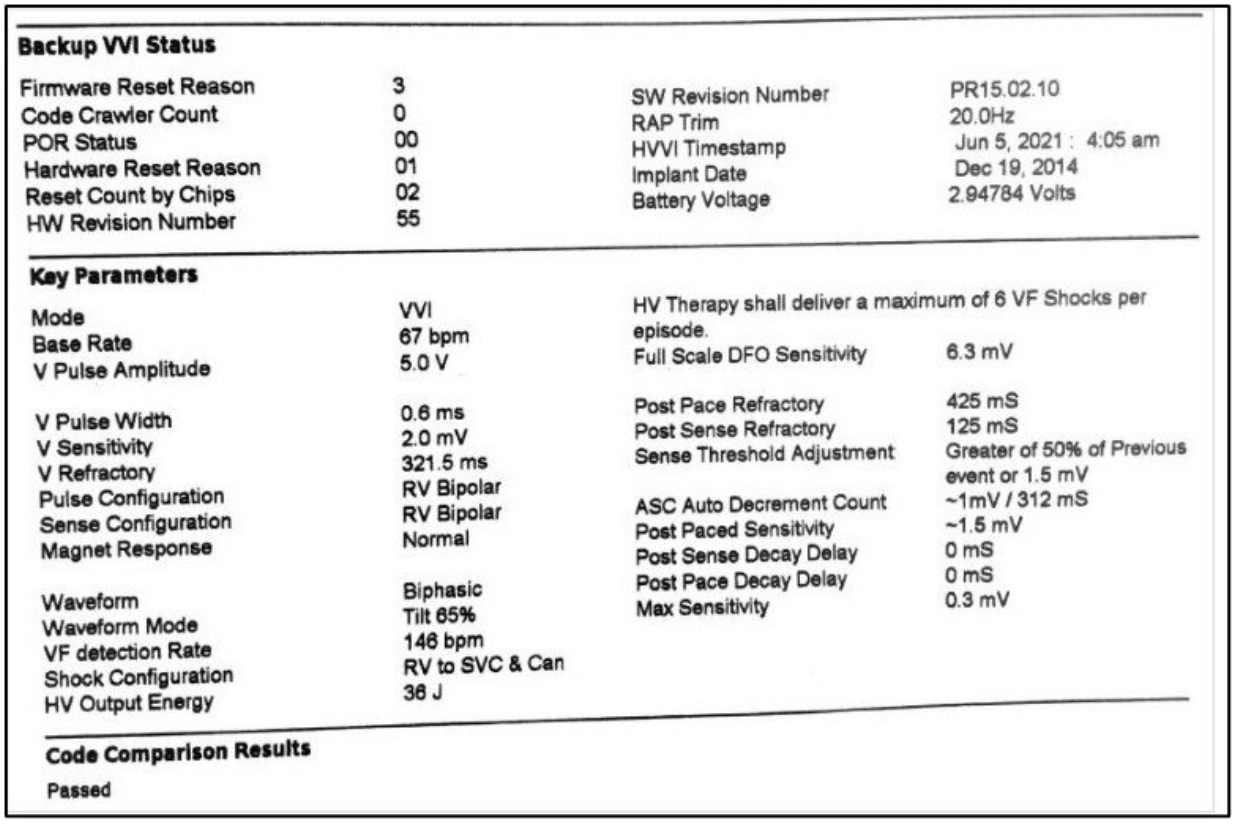
Without appropriate technical updates, patients are at risk of inappropriate shocks from their defibrillators

January 20 2022



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	Full Scale DFO Sensitivity	6.3 mV
V Pulse Amplitude	5.0 V		
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% of Previous event or 1.5 mV
Pulse Configuration	RV Bipolar	ASC Auto Decrement Count	~1mV / 312 mS
Sense Configuration	RV Bipolar	Post Paced Sensitivity	~1.5 mV
Magnet Response	Normal	Post Sense Decay Delay	0 mS
		Post Pace Decay Delay	0 mS
Waveform	Biphasic	Max Sensitivity	0.3 mV
Waveform Mode	Tilt 65%		
VF detection Rate	146 bpm		
Shock Configuration	RV to SVC & Can		
HV Output Energy	36 J		

Code Comparison Results

Passed

Device interrogation in the emergency department showed that the patient's defibrillator was in VVI backup mode with base rate of 67 beats per minute and ventricular fibrillation detection rate of 146 beats per minute. Credit: Heart Rhythm Case Reports

A case study of a patient who experienced inappropriate shocks from her defibrillator is presented in *Heart Rhythm Case Reports*, an official journal of the Heart Rhythm Society. This event likely took place because an FDA-recommended firmware update to strengthen cybersecurity had not occurred. This underscores the importance of upgrading firmware of Abbott devices according to FDA recommendations.

The patient, with an Abbott Fortify Assura implantable cardioverter-defibrillator (ICD) with a Merlin@home radiofrequency communicator, presented to the emergency department after receiving two shocks from her ICD without preceding symptoms. She had a history of atrial fibrillation with rapid ventricular response.

The patient was enrolled in at-home remote monitoring for her device and had frequent in-person device checks; however, the patient's device had outdated ICD firmware.

In August 2016, Muddy Waters LLC, an investment firm that conducts investigative research on public companies, released a report claiming that certain St. Jude Medical/Abbott cardiovascular implantable electronic devices (CIEDs) were vulnerable to cyberattack through the Merlin@home radiofrequency remote monitoring system, which allows care teams to review medical and technical information about the patient and the device without an in-person visit. Senior investigator Vineet Kumar, MD, FHRS, Division of Cardiac Electrophysiology, Inova Heart and Vascular Institute, Falls Church, VA, USA, explained, "Cyberattack of CIEDs could affect patients' confidentiality, interrupt remote monitoring, and even harm patients by changing device settings or promoting early battery depletion."

Consequently, St. Jude Medical/Abbott released a software patch for the radiofrequency communicator, which was successfully programmed

remotely into nearly 100% of actively used Merlin@home radiofrequency communicators. The company later released firmware updates to strengthen cybersecurity performance in the devices themselves. This requires an in-person visit to the healthcare provider, but it takes only three minutes to complete and is rarely associated with complications. Still, the firmware has only been updated in 24% of eligible devices. Because no harm is known to have been caused by a CIED cyberattack, deferring the firmware update may not have been prioritized for many patients. Additionally, reports have emerged showing that the firmware update may cause irreversible device malfunction with an incidence of 0.003%.

When the patient arrived at the emergency department, she was asymptomatic, and her vital signs were normal. Device interrogation demonstrated the ICD programming had reverted to backup mode, and thus no electrocardiograms were recorded during her shocks. Her device had several radiofrequency connection/disconnection events with the Merlin@home system over a short period of time. This was detected as a potential cyberattack and the device entered backup mode to avoid cybersecurity vulnerabilities due to event queue overload (EQO). In backup mode, the device is automatically reprogrammed to treat any heart rhythm with a rate over 146 beats per minute (BPM) with a shock. Based on the patient's history of atrial fibrillation with rates over 150 BPM, inappropriate treatment of atrial fibrillation with rapid ventricular response is the most likely cause of her ICD shocks.

EQO events occur most frequently in the setting of an updated Merlin@home software patch being used with outdated ICD firmware. This combination is currently in use in almost 75% of affected Abbott ICDs.

The patient's ICD was reprogrammed to the original settings, the cybersecurity firmware was upgraded, and she was released from the

emergency department.

"Physicians and their patients with affected Abbott devices now have another reason to consider updating their device firmware," said co-investigator Brett Atwater, MD, Director of Electrophysiology at Inova Heart and Vascular Institute in Falls Church, VA, USA. "While this is the first reported case, based on the reported frequencies of EQO events and the frequency of outdated firmware still in use in affected devices, other patients may experience similar events. This case highlights the importance of following FDA recommendations to update CIED firmware to protect not only against a cyberattack, but potentially even more importantly, to avoid unnecessary right ventricular pacing and ICD shocks."

The investigators recommend that the possibility of an inappropriate shock and/or unnecessary right ventricular pacing be incorporated into patient discussions about the risks and benefits of firmware update, to better assist shared decision making.

More information: Xiaoxiao Qian et al, Radiofrequency remote monitor software patch update without cybersecurity implantable cardioverter-defibrillator firmware update increases the risk of inappropriate implantable cardioverter-defibrillator therapies, *HeartRhythm Case Reports* (2022). DOI: 10.1016/j.hrcr.2021.12.016

Provided by Elsevier