Titre: Title:	Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)
Auteurs: Authors:	Mikaëla Ngamboé, Paul Berthier, Nader Ammari, Katia Dyrda et José M. Fernandez
Date:	2021
Type:	Article de revue / Journal article
Référence: Citation:	Ngamboé, M., Berthier, P., Ammari, N., Dyrda, K. & Fernandez, J. M. (2021). Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED). *International Journal of Information Security*, *20*(4), p. 621-645. doi:10.1007/s10207-020-00522-7

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/9257/
Version:	Version officielle de l'éditeur / Published version Révisé par les pairs / Refereed
Conditions d'utilisation: Terms of Use:	CC BY

Titre de la revue: Journal Title:	International Journal of Information Security (vol. 20, no 4)
Maison d'édition: Publisher:	Springer Nature
URL officiel: Official URL:	https://doi.org/10.1007/s10207-020-00522-7
Mention légale: Legal notice:	

International Journal of Information Security (2021) 20:621–645
https://doi.org/10.1007/s10207-020-00522-7

REGULAR CONTRIBUTION

Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)

Mikaëla Ngamboé[1] · Paul Berthier[1] · Nader Ammari[1] · Katia Dyrda[2] · José M. Fernandez[1]

Published online: 7 October 2020

Abstract

Cardiac implantable electronic devices (CIED) are vulnerable to radio frequency (RF) cyber-attacks. Besides, CIED communicate with medical equipment whose telemetry capabilities and IP connectivity are creating new entry points that may be used by attackers. Therefore, it remains crucial to perform a cybersecurity risk assessment of CIED and the systems they rely on to determine the gravity of threats, address the riskiest ones on a priority basis, and develop effective risk management plans. In this study, we carry out such risk assessment according to the ISO/IEC 27005 standard and the NIST SP 800-30 guide. We employed a threat-oriented analytical approach and divided the analysis into three parts, an actor-based analysis to determine the impact of the attacks, a scenario-based analysis to measure the probability of occurrence of threats, and a combined analysis to identify the riskiest attack outcomes. The results show that vulnerabilities on the RF interface of CIED represent an acceptable risk, whereas the network and Internet connectivity of the systems they rely on represent an important potential risk. Further analysis reveals that the damages of these cyber-attacks could spread further to affect manufacturers through intellectual property theft or physicians by affecting their reputation.

Keywords Cardiac implantable electronic device · CIED · Cybersecurity · Cyber-attack · Attack vector · Attack scenario · Threat-oriented analysis · Risk assessment

1 Introduction

Cardiac implantable electronic devices (CIED) have evolved from single-chamber pacing devices to resynchronization and defibrillation within the same device [1]. Modern CIED now include numerous functionalities being integrated into a single device, which has contributed to an increase in the number of implanted devices [2,3]. Besides, the use of telemetry-enabled CIED is increasing at the detriment of older models with no wireless communication capabilities [4,5], due to the significant advantages it brings to patient care [6,7]. For the remainder of this article, the acronym CIED will refer only to telemetry-enabled CIED.

CIED depend on a set of external systems to diagnose, monitor, and adjust patient therapy. These systems are: the *External programmer* used in the hospital, the *Home monitor* present at the patient's home, *Databases* housed either in the cloud or in servers located in the CIED manufacturer's network, and medical *Web applications*. Health professionals rely on the external programmer to obtain the programmed parameters of the patient, to adjust the desired therapies or to check the correct operation of the CIED [4,5]. The home monitor is used to periodically collect the data stored in the CIED and send them to a database. Thus, medical staff can access a patient's health information through a medical Web application, operated either by the CIED manufacturer or by a separate cloud service provider [6–8]. CIED communicate with the external programmer and the home-monitoring device via radio frequency (RF) signals transmitted in the Medical Implants Communication Services band (MICS 402-405 Mhz) [2,9–12], whereas they interact with the databases and the Web applications through the home-monitoring device and Internet protocol (IP) connectivity [6–8].

As evidenced by previous work, CIED are vulnerable to cyber-attacks that use their RF interfaces to communicate with the devices [13,14]. This is also true for non-telemetry-enabled CIED, but telemetry introduces additional vectors

✉ Mikaëla Ngamboé
mikaela-stephanie-2.ngamboe-mvogo@polymtl.ca

[1] École Polytechnique de Montréal, Montréal, QC, Canada

[2] Montréal Heart Institute, Université de Montréal, Montréal, QC, Canada

of cyber-attacks that can include manipulation of the home monitor, interception of transmissions from the home monitor to the cloud and the physician's station, and manipulation of the database [15,16]. Proof of the increased concern of cyber-attacks on CIED was given by the recall of almost half a million CIED by the Food and Drug Administration (FDA) in August 2017. According to the FDA, the aforementioned devices were vulnerable to unauthorized access, allowing a malicious person to reprogram them using commercially available equipment [17]. However, no such attacks have been reported. While we know it would be technically possible to conduct such an attack in the controlled environment of a research laboratory [13–15], it remains to be determined how viable such an attack would be on an actual target in the real world. This is precisely our research question: What are the real-life risks of cyber-attack onto telemetry-enabled CIED and the systems they depend on?

In this study, we carry out a realistic risk assessment of such attacks, with regards to actual impact these problems pose in terms of health, economy, quality of life, and privacy of the affected parties. The scope of our assessment is limited to the CIED and the systems on which they depend, i.e., the external programmer, the home monitor, the storage database to which the home monitor sends the data transmitted by the CIED, and the medical Web application that accesses this database. The risk is assessed under the guidelines of the ISO/IEC 27005 standard jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [18]. ISO/IEC 27005 defines the guidelines to be followed when managing the risks related to the security of information. Indeed, we start by identifying threats, then analyze, and finally assess them. We identify the threats through a literature review of potential cyber-threat sources (i.e., actors) and vulnerabilities affecting the systems under study. Risk is analyzed by performing the task on the National Institute of Standards and Technology (NIST) Special Publication 800-30 [19], a guide for conducting risk analysis. We used a threat-oriented analytical approach and divided our analysis into three parts: first, an actor-based analysis to determine the impact of the attacks; second, a scenario-based analysis to measure the probability of the threats; and third, a combined risk analysis to calculate the risk value associated with each threat. For the risk assessment, we classify the risk according to four levels of severity (unacceptable, undesirable, acceptable, and negligible) and then propose a risk management strategy (refuse, manage, and accept) for each level.

Our motivation to conduct this research is based on the need to understand the real scope of the problem. After the FDA statement was released, patients began to massively call their cardiologists to get an explanation about these potential failures and to what extent they were in danger. It is at times difficult for physicians to answer them, since cybersecurity is not their field of expertise and because there is little information about the clinical impact of the exploitation of the vulnerabilities found. This is why we believe that such a "reality check" is necessary, as the real scope of the problem is not clear at all. By determining the scope of the problem, we contribute to (1) extend the knowledge of the threats affecting CIED, (2) provide guidance on which threats should be addressed in priority, and consequently (3) provide to the organizations potentially interested in this kind of risk assessment a basis from where to start, e.g., health regulation agencies, device manufacturer, health practitioners, etc.

2 Methodology

2.1 Aim of the risk assessment methodology

The number of implantable medical devices (IMD) that rely on Information and Communications Technology (ICT) to ensure patients therapy, diagnosis, or follow-up is increasing. However, unlike traditional ICT systems (computers, servers, networks, etc.), relatively little attention has been given to practical risk assessment studies on IMD. Indeed, even though the first vulnerabilities in IMD were found in 2008, it is only in 2015 that the first IMD cybersecurity risk assessments [20] appear in the literature. Since then, few cybersecurity risk assessment methodologies tailored specifically for IMD have been proposed and, as we will discuss in Sect. 6, continue to present important limitations in terms of assessment of real-world impact and threats.

In this work, we propose a method for assessing the cybersecurity risk incurred by CIED, a subcategory of IMD. Our method can be used to guide organizations interested in conducting risk assessments of CIED and can be extended to other IMD.

2.2 Definitions

We define here the cybersecurity and risk assessment terms used in this article.

Actor A person or organization that violates the integrity, privacy, or confidentiality of a computer system's data to obtain a benefit.

Impact Quantification of an attack's effect or consequence on the target or victim.

Victim A person or organization that is the subject of a computer attack.

Attack goal Final effect desired by the actor, resulting in a negative impact on the target system or victim.

Scenario Set of actions carried out by the actor to achieve his attack goal.

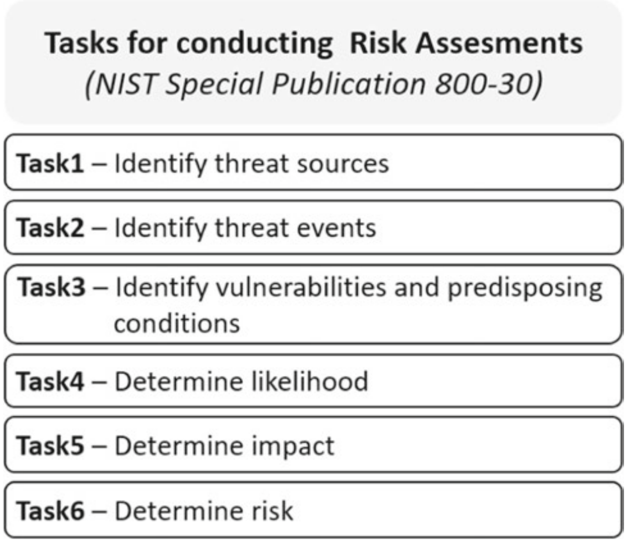
Tasks for conducting Risk Assesments
(NIST Special Publication 800-30)
Task1 – Identify threat sources
Task2 – Identify threat events
Task3 – Identify vulnerabilities and predisposing conditions
Task4 – Determine likelihood
Task5 – Determine impact
Task6 – Determine risk

Fig. 1 NIST Special Publication 800-30 tasks to conduct risk analysis

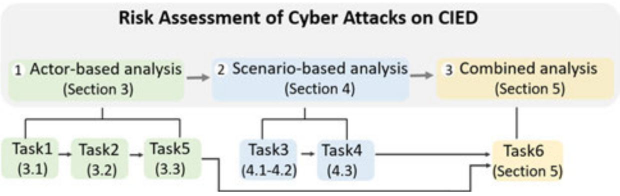
Risk Assessment of Cyber Attacks on CIED
1 Actor-based analysis (Section 3)
2 Scenario-based analysis (Section 4)
3 Combined analysis (Section 5)
Task1 (3.1)
Task2 (3.2)
Task5 (3.3)
Task3 (4.1-4.2)
Task4 (4.3)
Task6 (Section 5)

Fig. 2 Methodology

Threat A combination of a person with deliberate intent (actor) committing acts in particular fashion (scenario), resulting in a negative consequence (impact).

Vulnerability A design, manufacturing, or programming flaw in a system that may offer the opportunity to conduct an attack on it.

Attack vector Subset of vulnerabilities for which there is a demonstrated attack method by which the vulnerability is employed (exploited) by the actor to reach its final goal or an intermediate goal toward it (e.g., gaining access).

Exploit Subset of attack vectors related to software vulnerabilities.

Probability Likelihood that a particular threat (a given actor successfully reaching an attack goal through a given scenario) be materialized during a given period of time.

Risk Quantification of a threat (Risk = Impact∗Probability).

2.3 Risk assessment methodology

The risk assessment has been performed according to the ISO/IEC 27005 standard for information security risk management. Indeed, potential threats (actors and scenarios) are identified, then their impact and probability of occurrence are analyzed, and finally, the risk is assessed based on a severity rating. Our analytical method is threat-oriented which means that it "starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent" [19]. We have chosen this approach because it meets our objective of determining the severity of threats, i.e., actor–scenario pairs. Furthermore, the ISO/IEC 27005 standard gives guidelines but does not specify the exact way to conduct a risk analysis. For this purpose, we employed the Special Publication 800-30, a guide developed by the NIST for conducting risk analysis. This guide contains the tasks to be performed when conducting a risk analysis (Fig. 1), we have adapted these tasks to our needs and divided the analysis into three steps (Fig. 2):

Step 1. Actor-based risk analysis In this phase, we aim to determine and quantify the impact of attacks on the CIED ecosystem. To do this, we first identify potential actors that would be interested in attacking the CIED ecosystem. Then, we determine their likely attack goals and from there we quantify the impact on the victim of the successful accomplishment of such attack goals. We do this separately according to four different categories of impact: health, monetary, quality of life, and privacy. We measure the impact on health by applying the Hayes classification approach [21] that was introduced to classify the impact of different levels of clinically significant electromagnetic interference with pacemakers. The monetary, quality of life, and privacy impacts are measured using the Fair Information Practice Principles 199 (FIPPS 199) [22] from NIST. The FIPPS 199 is a standard for assessing the security of information systems. The impact is quantified according to a four-level scale described in Table 1 and discussed in more detail in Sect. 3.3.

Step 2. Scenario-based risk analysis Here, we estimate the probability of occurrence of various threats. We start by identifying attack vectors, i.e., exploitable vulnerabilities, associated with CIED. We found those attacks vectors on the literature [13–15,23], the ICS-CERT advisories [24–26], the National Vulnerability Database (NVD) maintained by the NIST, and the Common Vulnerabilities and Exposure (CVE) database maintained by the Mitre Corporation [27–34] . Next, we describe how these attack vectors can be strung together into a series of actions, i.e., attack scenarios, that lead to the achievement of the attack goals (determined in Step 1). Once this is done, we calculate for each threat, i.e., each (actor, scenario) pair, its probability of occurrence according to the formula

$$P = c * o * m \tag{1}$$

where c, o, and m represent, respectively, an assessment of the actor's *capacity*, *opportunity*, and *motivation* to conduct the attack scenario described. More precisely, capacity takes into consideration the technical complexity of the attack scenario and the technical and material resources available to the actors to carry it out. The opportunity represents the actor's chances of having physical or network access to the target and being there at the right time to exploit an attack vector and conduct subsequent scenario actions. Finally, motivation captures the inherent likelihood that the actor will put the resources in place and attempt to conduct the attack scenario given what he stands to gain from successful accomplishment of the attack goal.

Step 3. Combined risk assessment In this last step, we calculate the overall risk associated with each attack scenario based on the most likely actor.

$$R = I * P_{\mathrm{MAX}} \tag{2}$$

where I is the impact calculated from Step 1 and P_{MAX} is the maximum actor probability for each attack scenario, as determined in Step 2.

3 Actor-based analysis

3.1 Potential actors

To our knowledge, apart from some laboratory experiments and proofs of concept, no real attacks have taken place against CIED or the devices they depend on. Therefore, the groups of actors (i.e., attackers) who could exploit these devices for malicious purposes have not yet been fully identified. Aware that CIED are cyber-physical systems involving IT and physical aspects, both aspects should be considered when discerning who the actors could be. Until now, cyber-attackers have exploited IT systems to make money, obtain information, conduct sabotage activities, or create disinformation and degrade confidence in governments and other kinds of subversive political actions. However, in the case of cyber-physical systems in general, and IMD in particular (including CIED), we should consider another type of motivation, namely the possibility of physically harming individuals by leveraging the hardware component of the devices. In this line of thought, we can distinguish two categories of actors. On the one hand, we consider the traditional cyber threat actors defined by the ICS-CERT, for which the targets are the IT systems. On the other hand, we have those hackers that may have been hired by assassins or directly by those having a motivation to inflict harm or even a particular victim; we refer to this (combined) threat actor as *assassins for hire*.

Concerning threats on traditional IT infrastructure, experts in cybersecurity have developed a good understanding of threat actors, including their typical behavior and attack methods. This has led to some capacity in predicting and thwarting some of their actions. The study, analysis, and reproduction of the various modalities of computer attacks that have been perpetrated in the past and are still being perpetrated today have contributed to this situation. However, this is not the case of assassins for hire in the context of CIED, which to this date remains a possibility that has not yet been materialized. Consequently, there have been few attempts to evaluate the risk that this possibility represents given the lack of evidence of real attacks. Nonetheless, the proliferation of cyber-physical systems and particularly those used for therapeutic purposes makes it necessary to conduct such studies.

The ICS-CERT has characterized a *cyber threat source* as "persons who attempt unauthorized access to a control system device and/or network using a data communications pathway" [35]. It further classifies this threat source into four groups (A1 through A4):

A1. *Cybercriminals groups* This includes traditional cybercriminals groups that use compromised computer systems to commit identity theft and online fraud of various kinds, mostly for monetary gain.

A2. *Industrial spies* Organizations that use computer tools to illegally acquire intellectual property, know-how, trade, and commercial secrets, or other kinds of corporate confidential information. This kind of espionage occurs between competing corporations, for economic reasons.

A3. *Foreign Intelligence Agencies* Foreign state-based organizations that use computer tools to acquire sensitive information on opposing states, corporations, or individuals, or otherwise influence their actions.

A4. *Terrorist groups* Organizations seeking to create public disorder or sow national terror, by committing destructive violent acts.

While this taxonomy of cyber threat sources was introduced for traditional threats to purely IT infrastructure, we nonetheless proposed to use it in the context of cyber threats against the CIED ecosystem as well, since this ecosystem is composed of both IT elements and of cyber physical systems that have an IT component.

Nonetheless, this taxonomy is not complete in the context of threats against IMD. As we discussed above, the possibility of inducing harm or even death motivates the addition of a new threat group, i.e., assassins for hire. In coming up with a profile for these assassins for hire, it is necessary to analyze simultaneously those who execute the attack (the assassin and the hacker, which might be the same person) and those who hire their services (the client). We will start

Table 1 Impact levels

Type	Level	Description of the impact	Victim
Health	1	Minor harm	Patient
	2	Significant harm not involving life-threatening injuries	
	3	Severe harm that involve life-threatening injuries	
	4	Catastrophic harm that involve loss of life	
Monetary	1	Minor monetary loss	Manufacturer
	2	Significant monetary loss	Health center
	3	Severe monetary loss	
	4	Catastrophic monetary loss	
Quality of life	1	Minor damage on quality of life	Patient
	2	Significant damage on quality of life	
	3	Severe damage on quality of life	
	4	Catastrophic damage on quality of life	
Privacy	1	Minor damage on privacy if information disclosure	Patient
	2	Significant damage on privacy if information disclosure	Manufacturer
	3	Severe damage on privacy if information disclosure	Health center
	4	Catastrophic damage on privacy if information disclosure	

with the client. We suppose that he is a person with elevated economic means and high motives to hire an assassin. His motives can be varied: passional, ideological, economic, etc. As far as the hacker is concerned, we suppose that he is an experienced person, highly competent and that he enjoys a certain prestige in his sector. He executes the crime for purely economic reasons and accepts those contracts he knows he can carry out successfully since success is what makes his prestige.

A5. *Assassin for hire* a assassin/hacker hired by a third party to harm the life of an individual. He maliciously exploits cyber physical systems for economic reward.

Considering the likely objectives [36] and motivations [35] of these actors, we maintained the five kinds of attack goals (G1 through G5) described herein.

3.2 Attack goals

3.2.1 G1: Access patient's sensitive data

CIED ecosystem devices are an attractive target because they constitute a rich source of information for several types of actors. Beyond medical data, they store other types of information such as email addresses, residence addresses, telephone numbers, and social security numbers. On the one hand, intelligence services (A3) and terrorist groups (A4) would be interested in having this information because it would allow them to attain their ultimate goal (surveillance, assassination, etc.). On the other hand, cybercriminal groups (A1) would be interested to leverage this information to obtain monetary gain since the medical data of individuals are highly valued in the black market [37–40]. Their clients could be, for example, insurance companies (medical or automotive) that may use this information to assess the cost of insurance premiums or simply refuse coverage.

3.2.2 G2: Gain knowledge of device operation and software

There is significant competition between medical device manufacturers because of its high profit margins and high barriers to entry in the market [41,42]. Accordingly, CIED ecosystem devices could be a target for industrial spies (A2) aiming to obtain intellectual property on device design, software, and other kinds of engineering details. Subsequently, such information could be sold to competing medical device manufacturers or possibly to counterfeit medical device manufacturers in less regulated countries (similarly to the production of counterfeit or generic pharmaceutical products). Furthermore, this information is also valuable for criminal groups (A1), intelligence services (A3), and terrorist groups (A4) because it allows them to undertake attacks by maliciously exploiting the device characteristics or operating mode.

3.2.3 G3: Induce medical staff to make errors

Health is one of the main factors of concern for individuals. Hospitals and their personnel are highly valued in society because individuals trust them [43–46]. Some attackers may be interested in damaging the reputation of health centers or professionals to sow distrust and fear in the society. These could include foreign intelligence services (A3), terrorist groups (A4), or even cybercriminal groups (A1). Besides, foreign intelligence services (A3), terrorist groups (A4), and assassins for hire (A5) could be interested in harming a particular, targeted person. Thus, inducing medical staff to make errors not only would they be achieving their goal, but they would also be evading the responsibilities of their actions by making their interference less detectable

3.2.4 G4: Alter device behavior to endanger patient

This constitutes the most potentially worrisome outcome of the cyber-attack against the CIED ecosystem. Indeed, by changing the device settings so that it has an unexpected or dangerous behavior, actors could seriously endanger a patient's life. It is conceivable that foreign intelligence services (A3), terrorist groups (A4), and assassins for hire (A5) targeting particular high-value or highly visible individuals might be motivated to use this kind of attack for assassinations or as a form of extortion or ransom.

3.2.5 G5: Alter device behavior to decrease quality of life

For the same reasons described above, intelligence services (A3) and terrorist groups (A4) could be motivated to use similar methods to accomplish non-lethal disruptive effects on patients by forcing them to repeatedly visit the clinic due to device malfunction, generate false alarms, or otherwise tampering with device configuration. Beyond serious harm, such disruptions could be used to undermine the confidence of the population on health providers, device manufacturers, or create panic and terror (A3 and A4). The possibility should also be considered that cybercriminals (A1) migrate from traditional forms of IT-based extortion, such as file-encrypting ransomware, to medical device-based extortion, e.g., by locking out access by health practitioners to a patient's CIED and demanding a ransom to restore it.

In summary, the vulnerability of the CIED ecosystem to cyber-attacks is a matter of concern not only for patients but also for other groups such as health practitioners, medical device manufacturers, and government in general.

3.3 Impact of attack goals

Independently of the various actors' goals and motivations, these attacks will have an impact on the victim, whether the patients themselves or those other groups affected. In order to account for the various types of consequences that these attacks could have on them, we measure impact according to four separate aspects: health (H), monetary (M), privacy (P), and quality of life (QL). We chose these four factors because affecting them negatively aligns precisely with the attack goals we have previously discussed in Sect. 3.2. Furthermore, by separating our analysis for these factors, we aim to support different agendas and objectives of those organizations potentially interested in this kind of risk assessment, e.g., health regulation agencies, device manufacturers, health practitioners, etc. The impact scale ranges from 1 to 4, with 4 being the highest impact level (most severe). The description of the impact levels is given in Table 1, and the summary of the analysis is presented in Table 2. The explanation of the impact analysis by attack goal follows.

G1 (P) While confidential, the information disclosed would not have severe consequences (except maybe in terms of insurability) and is likely to exist in other or be otherwise available to actors through other sources or other more traditional forms of cyber-attacks no related to CIED. (M) The disclosure of this information may be grounds for legal action against the hospital and the manufacturer.

G2 (M) The medical device industry is very profitable, and competition between manufacturers is fierce. Losses due to intellectual property theft could reach tens of millions of dollars.

G3 (H) We consider the worst-case scenario: the dependent patient (i.e., one that cannot survive without the device) for whom the doctor does not make the appropriate diagnosis potentially leading to loss of life. (M) The doctor and hospital could face severe penalties. (QL) The patient's quality of life would be affected if G3 is achieved.

G4 (H) Worst-case scenario, death of dependent patients. (M) In the event of a legal action, the company could face significant economic penalties. Moreover, the manufacturer could lose market share or have its devices removed from the market by regulators.

G5 (M) The equipment could be removed from the market, causing economic losses to the company. (QL) The patient would feel a temporary discomfort.

4 Scenario-based risk analysis

4.1 Vulnerabilities

We now inventory the vulnerabilities (V_i) affecting the CIED ecosystem. We have harvested this information from several sources, including ICS-CERT advisories, the NVD maintained by the NIST, the CVE database maintained by the Mitre Corporation and previous research in this area [13–15,23]. We separated the vulnerabilities in three groups, depending on what devices they affect, with some of them applicable to more than one type of device (i.e., V_9, V_{10}). We

Table 2 Impact results by attack goal

Attacks goal	*H*	*M*	QL	*P*
G1 Access patient's sensitive data	–	1	–	2
G2 Gain knowledge of device operation and software	–	4	–	–
G3 Induce medical staff to make errors	4	3	1	–
G4 Alter device behavior to endanger patient	4	3	–	–
G5 Alter device behavior to decrease quality of life	–	2	2	–

have inventoried 15 vulnerabilities, enumerated in Table 3; a more detailed explanation of the vulnerabilities can be found in "Appendix B."

4.2 Attack scenarios

Once we have identified who the actors are and what they are trying to achieve (attack goals), we are now interested in the strategy that it is going to be used by them, i.e., how will they exploit the vulnerabilities of the CIED ecosystem to achieve their goals? Thus, as illustrated in Table 4, an attack goal can be achieved through different scenarios. As defined in Sect. 2.2, an attack scenario is the sequence of events that must occur for the attack to take place.

It can be noticed that the same scenario can serve to achieve different attack goals. Since a threat is a pair (actor, scenario) and the actors can vary from one attack goal to the next, we carried out the scenario-based risk analysis by attack goals. The explanation of the scenarios of each attack goal follows. For a more extensive description of the sequence of events leading to the achievement of the attack scenarios, refer to C.

4.2.1 G1: Access patient's sensitive data

There are at least three ways to acquire patient's medical data: performing a radio attack (S_1, S_2) on the incoming RF communication between the CIED and the external devices (monitor, programmer), getting unauthorized physical access to the monitor contents (S_3) or performing a network attack on the monitor (S_4).

Executing the radio attacks described in Scenarios S_1 and S_2 requires the actor to have specialized materials and software, namely an software-defined radio (SDR), an antenna, and a radio signal processing software (e.g., GNURadio, HackRF, etc.). Once this requirement has been met, the actor must go either to the patient's home (S_1) or to the hospital (S_2), place himself at a distance relatively close to the CIED, configure its antenna in reception mode, tune it to the transmission frequency of the CIED then, record the signals emitted by the latter, and read the patient's medical data by exploiting the CIED unencrypted data storage and transmission vulnerability (V_3).

The physical attack of Scenario S_3 also requires the actor to have specialized equipment. An in-debugger-circuit, a debugger IDLE, and a pirate bus (or an F to F jumper wire) are needed. Since the monitor is the targeted device, the actor must go to the patient home and then connect to the device's debugging interfaces employing the pirate bus (or the F to F jumper wire). After that, he must use the in-debugger-circuit along with the debugger IDLE to access the monitor's memory content. Consequently, the actor must exploit the following three vulnerabilities of the monitor: exploiting debugging interfaces (V_{10}), server hardcoded authentication credentials (V_{13}), and hardcoded server parameters (V_{14}).

The monitor is once again the target device in Scenario S_4. Here, the network attack proposed relies on installing a backdoor on the device. In this case, the actor must know beforehand the day when an update will take place. Once done, he must approach the patient's home then, access the patient's private network, and achieve a man-in-the-middle attack exploiting the monitor's remote firmware update session (V_{15}). At that point, the actor must swap the updated firmware for a backdoor. Thus, he will be able to access the target at any later time employing the backdoor.

4.2.2 G2: Gain knowledge of device operation and software

G2 can be achieved by performing network attacks on the external devices (S_4, S_6, S_7, or S_8), launching a Web attack on the programmer software deployment network server (S_5), or getting unauthorized physical access to the external devices (S_9, S_{10}). In the last case, we will talk about a physical attack on the external devices.

For the network attacks of Scenarios S_4, S_6, S_7, and S_8, the actor must either go to the patient's home (S_4, S_7) or the hospital (S_6, S_8). Note that for Scenarios S_4 and S_7, this must occur the day of an update of the monitor and the programmer, respectively. Once on the crime scene, the actor should access either the targeted device network (S_7, S_8) or the communication channel established between the communicating parties (S_4, S_6). In the last case, the communicating parties are the external device and the Web server of the entity in charge of the updates. Thus, once in the external device network the actor should either connect himself to the USB port

Table 3 List of vulnerabilities

Vulnerability description	
CIED	
V_1	Weak authentication algorithms
V_2	Boundless telemetry session duration
V_3	Unencrypted data storage and transmission
V_4	Lack of command whitelisting techniques
Programmer	
V_5	Unencrypted hardcoded authentication credentials
V_6	Software directory path traversal
V_7	Improper restriction of communication channel
V_8	Unprotected removable media/hard drives
V_9	Unprotected USB serial port connections
V_{10}	Exploiting embedded debugging interfaces (Joint Test Action Group (JTAG) and Universal Asynchronous Receiver–Transmitter (UART))
Monitor	
V_9	Unprotected USB serial port connections
V_{10}	Exploiting embedded debugging interfaces (JTAG and UART)
V_{11}	OS hardcoded authentication credentials
V_{12}	Exposed dangerous methods or functions
V_{13}	Server hardcoded authentication credentials
V_{14}	Hardcoded server parameters
V_{15}	Exploiting remote firmware update

Table 4 Attack scenarios

Attack goal	Scenario	Scenario description	Method
$G1$	S_1	CIED-Monitor communication interception	Intercepting RF signals with an SDR
	S_2	CIED-Programmer communication interception	Intercepting RF signals with an SDR
	S_3	Extraction of health data stored into the monitor	Connecting to the debugging ports
	S_4	Insertion of a backdoor (malware) into the monitor	Performing MITM attack during a firmware update session
$G2$	S_4	Insertion of a backdoor (malware) into the monitor	Performing a MITM attack during a firmware update session
	S_5	Extraction of the programmer's system data from the device's SW deployment network server	Sending a malicious http request to the server
	S_6	Extraction of the programmer's system data	Accessing the device through an update session communication channel
	S_7	Reading/extraction of the monitor file system	Accessing the device USB port
	S_8	Reading/extraction of the programmer file system	Accessing the device USB port
	S_9	Reading/extraction of the programmer system data	Removing the media device hard drive
	S_{10}	Reading/extraction of the monitor OS information	Connecting to the debugging ports
$G3$	S_{11}	Insertion of a malware that produces programmer reading errors	Performing a MITM attack during an update session
	S_{12}	Introduction of calibration errors into the CIED microprocessor (through malware insertion or sending inappropriate commands)	Sending RF commands with an SDR
	S_{13}	Insertion of a malware that produces programmer reading errors	Using the device USB port
$G4$	S_{11}	Insertion of a malware that ignores programmer therapy settings	Performing a MITM attack during an update session
	S_{11}	Insertion of a malware that makes programmer apply a predefined dangerous treatment	Performing a MITM attack during update session
	S_{11}	Insertion of a backdoor (malware) into the programmer	Performing a MITM attack during a session update
	S_{12}	Modification of the CIED section of RAM containing the therapy code to be applied to the patient	Sending RF unauthorized commands with an SDR
$G5$	S_{10}	Disable the periodic data transmission from the monitor	Connecting to the debugging ports
	S_{11}	Insertion of a malware that produces programmer's reading errors	Performing a MITM attack during an update session
	S_{14}	Maintain a CIED's telemetry session indefinitely open	Sending RF commands with an SDR

and acquire the file system (S_7, S_8) or have direct access to the devices and therefore to the data (S_4, S_6).

In Scenario S_5, the actor must find the URL from which the programmer update application retrieves files from the server of the software deployment network. Once this is done, he modifies the URL with commands and Web server escape code. After that, he sends this URL to the Web server through a Web request. Thus, if the attack is successful, the actor will be able to extract the desired files.

We can thus observe that the attacks set up in the above-mentioned scenarios fall into the category of cyber steal attacks as defined in the taxonomy AICan (Availability Integrity Confidentiality anomalies) [47].

Getting unauthorized physical access to the external devices (S_9 and S_{10}) is another means to achieve G2. On Scenario S_9, the extraction of the programmer hard drive is required. Thus, the actor should go to the hospital and remove it. As far as Scenario S_{10} is concerned, the attack is on the monitor, that is to say that the crime scene is the patient's home. The sequence of events of this scenario is that of S_3 except that two events are added, namely (1) connect to the debug port of the operating system and then (2) authenticate using the credentials that will have been previously acquired by performing the same actions as in S_3.

4.2.3 G3: Induce medical staff to make diagnostic errors

G3 can be achieved by three kinds of attacks: a network attack on the programmer (S_{11}), a radio attack on the CIED (S_{12}), or physical attacks on the programmer (S_{13}). The sequence of events for Scenario S_{11} is practically the same as that for Scenario S_4. What differentiates both scenarios is the target device. In S_4, it is the monitor, while in S_{11}, it is the programmer. Thus, the only difference between S_{11} and S_4 stems from the first event, that in the case of S_{11} is happening in the patient's home.

Scenario S_{12} is completely similar to Scenarios S_1 and S_2. The only change is the actor's behavior. Indeed, in Scenarios S_1 and S_2 he intercepts data; he is a passive actor. In Scenario S_{12}, however, he transmits data; thus, he is an active actor. The events in Scenario S_{12} are otherwise practically the same as in S_1 and S_2. We say practically because first, a new event is added. That is the transmission of data. Second, one of the events of S_1 and S_2 is modified. We saw for the G1 scenario the actor would have to configure his antenna in reception mode to intercept the data, while in S_{12} it will have to put in transmission mode.

In Scenario S_{13}, a network attack is performed on the programmer. The actor's purpose here is to introduce a calibration error on the device, by inserting a malware through the device's USB port connection. To do so, he goes to the patient's home, accesses the patient's network, scans the network ports to find the one that corresponds to the USB connection, and then sends the malware through the aforementioned port. As can be noticed, the sequence of events for Scenario S_{13} is quite similar to that of Scenario S_8. The difference between both is the last event which in Scenario S_8 is accessing the device file system, while in Scenario S_{13} it is sending the malware.

4.2.4 G4: Alter device behavior to endanger patient

G4 is achievable by perpetrating network attacks on the programmer (S_{11}). These attacks can take several forms as detailed in Table 4. Indeed, the actor can implement these scenarios to send malicious code that ignores the therapy settings set by the practitioners, or introduces a calibration error into the device, or allows him to access the device through a backdoor. Performing a radio attack against the CIED (S_{12}) is another way to accomplish the Goal G4. The actor's purpose here will be to modify the device's RAM section containing the therapy code to be applied to the patient. As those scenarios have already been appearing in the attack goal G3, the event sequence will be the same.

4.2.5 G5: Alter device behavior to decrease quality of life

Three kinds of attacks can be carried out to achieve attack Goal G5. The first one, S_{10}, consists of perpetrating a physical attack on the monitor to disable the device's periodic data transmission. The second one, S_{11}, relies on the execution of a network attack on the programmer. The actor introduces a calibration error on the device by inserting malware. The third one, S_{14}, is a radio attack on the CIED. The goal will be to maintain a wireless communication session indefinitely open by sending RF wake-up commands. The event sequence is similar to that of Goal G4.

4.3 Probabilities of occurrence

As defined in Sect. 2.2, the probability of occurrence (P_r) represents the chance that a given threat (actor–scenario pair) materializes. In other words, it is the likelihood that an actor achieves an attack scenario with success. By success, we mean the achievement of the attack's goal or what is the same, the engendering of a specific impact on the victim. We calculate the probability by threat. That is, for each actor of each scenario. As explained in the Methodology section (Sect. 2.3), P_r is calculated (1) as the multiplication of the three actors attributes: capacity (c), opportunity (o), and motivation (m). The c, o, and m values vary from 1 to 4, with 4 corresponding to a higher likelihood. In the following paragraphs, we justify the rates assigned to c, o, and m for each threat, with the overall P_r values given in Table 5.

Table 5 Probability of occurrence of identified threats

Attack goal	Scenario	Actor	c	o	m	P_r
$G1$	S_1	A3	3	2	2	12
		A4	3	1	1	3
	S_2	A3	3	2	2	12
		A4	3	2	1	6
	S_3	A3	2	2	2	8
		A4	1	1	1	1
	S_4	A3	4	2	2	24
		A4	3	1	1	3
$G2$	S_4	A1	4	1	2	8
		A2	4	2	4	32
		A3	4	2	3	24
		A4	3	1	3	9
	S_5	A1	4	3	2	24
		A2	4	3	4	48
		A3	4	3	3	36
		A4	3	3	3	27
	S_6	A1	4	1	2	8
		A2	4	2	4	32
		A3	4	2	3	24
		A4	3	1	3	9
	S_7	A1	4	2	2	16
		A2	4	3	4	48
		A3	4	3	3	36
		A4	3	2	3	12
	S_8	A1	4	3	2	24
		A2	4	3	4	48
		A3	4	3	3	36
		A4	3	3	3	27
	S_9	A1	4	1	1	4
		A2	4	2	1	8
		A3	4	2	1	8
		A4	4	1	1	4
	S_{10}	A1	1	1	1	1
		A2	2	2	1	4
		A3	2	2	1	4
		A4	1	1	1	1
$G3$	S_{11}	A1	4	1	1	4
		A3	3	2	3	18
		A4	3	1	3	9
		A5	3	2	4	24
	S_{12}	A1	2	1	1	2
		A3	2	2	3	12
		A4	2	1	3	6
		A5	2	2	4	16
	S_{13}	A1	4	3	1	12
		A3	3	3	3	27
		A4	3	3	3	27
		A5	3	3	4	36
$G4$	$S_{11(a)}$	A3	3	2	2	18
		A4	3	1	3	9
		A5	4	2	4	32
	$S_{11(b)}$	A3	2	2	2	8
		A4	1	1	3	3
		A5	2	2	4	16
	$S_{11(c)}$	A3	3	2	2	12
		A4	3	1	3	9
		A5	4	2	4	32
	S_{12}	A3	2	2	2	8
		A4	2	1	3	6
		A5	2	2	4	16
$G5$	S_{10}	A1	1	1	1	1
		A3	2	2	3	12
		A4	1	1	3	3
	S_{11}	A1	4	1	1	4
		A3	3	2	3	18
		A4	3	1	3	9
	S_{14}	A1	3	1	1	3
		A3	3	2	3	18
		A4	3	1	3	9

4.3.1 Attack goal G1

Capacity Scenarios S_1 and S_2 are accomplished by means of radio attacks. The capacity for Actors A3 and A4 are the same ($c = 3$) for many reasons: The knowledge is abundant and accessible to all the actors; the software tools used to intercept and process RF signals are increasingly simpler to use, thus reducing the attack's technical difficulty; and the equipment needed to perform these attacks (SDR and antenna) is not expensive. For Scenario S_3, even if the knowledge is accessible to all the actors and the equipment needed to conduct the attack is not expensive, the attack is technically complex to achieve. Indeed, it involves the exploitation of two vulnerabilities for which solid knowledge of computer programming and architecture is required. Normally, Actor A3 recruits experts with exceptional technical skills and have more human resources. They have more capacity than Actor A4. Thus, in Scenario S_3 A3 capacity ($c = 2$) is higher than the one of Actor A4 ($c = 1$). Scenario S_4 is a network attack, and thus additional material is not required. Additionally, there is nowadays extensive information available and tools to perform the attack in S_4. Thus, capacity for Actors A3 and A4 will be the same ($c = 3$) in this scenario.

Opportunity In Scenarios S_1 and S_3, the attack takes place in the patient's home. In these cases, Actor A3 ($o = 2$) has a better chance than Actor A4 ($o = 1$) since they are specifically trained to infiltrate private sites without being noticed. In Scenario S_2, the attack takes place in the hospital during a patient's medical visit. The latter implies that adversaries only have approximately two days a year to conduct the attack, coinciding with the number of times patients go to the doctor. However, since hospitals are public places, the actors are less likely to be noticed. Thus, the opportunity score for Actors A3 and A4 ($o = 2$) is the same. In Scenario S_4, the attacks take place during a monitor's update session, which takes place only about once a year. Actor A3 access to this information and opportunity to leverage it is greater ($o = 2$) than that of Actor A4 ($o = 1$).

Motivation Both Actors A3 and A4 benefit from the crime. They gain access to sensitive personal information. For A3, this attack objective is in line with the *raison d'tre* of their profession, i.e., obtaining private information from individuals. Thus, the motivation of Actor A3 ($m = 2$) will be higher than that of Actor A4 (m =1) because for A3 this attack objective is an end in itself, while for A4 it is a means to an end (sow national disorder).

4.3.2 Attack goal G2

Capacity In Scenario S_5, a Web attack is launched. There is information and tools available online to perform this kind of attack. Actor type A4 are experts in the field (Web attack). On the other hand, Actors A2 and A3 are specialists in the extraction of information from people or systems. Besides, they often have specialized human resources. Thus, the capacity of Actors A1, A2 and A3 ($c = 4$) is the same and it is higher than that of Actor A4 ($c = 3$). In Scenarios S_4, S_6, S_7, and S_8, network attacks are conducted. Once more, information and tools are available to achieve these attacks (i.e., network attacks). Actors A1, A2, and A3's capacity ($c = 4$) is higher than that of Actor A4 ($c = 3$) because either they have more know-how in malware development (A1) or their have specialized human resources (Actors A3 and A4). The attack performed in S_9 has no major technical complications. It is necessary to remove a hard disk and then mount it in another computer media. Thus, the capacity of all actors will be the same ($c = 4$). However, the achievement of Scenario S_{10} presents a major challenge. On the one hand, solid technical knowledge of computer programming and architecture is necessary. Also, there is no extensive information about how to realize the exploit in Scenario S_{10} . Thus, Actors A2 and A4's capacity ($c = 2$) is higher than that of Actors A1 and A4 ($c = 1$) since Actors A2 and A3 normally are experts with exceptional technical skills and have more human resources.

Opportunity Scenario S_5 is a Web attack where there is no restriction of time and space. So the actors' opportunity will be higher and the same ($o = 3$). Scenarios S_6 and S_4 take place during targeted device update sessions, during which there are constraints in terms of time (update session) and space (near the patient's home or hospital). As far as the time constraint is concerned, Actors A2 and A3 have better possibilities to know when an update session will take place. In terms of space constraint, Actors A2 and A3 have the same opportunities either at the patient's home or in the hospital. However, Actors A1 and A4 will have more chances in the hospital as this is a public place where they can go unnoticed. Thus, on the S_6 and S_4 Scenarios, Actors A2 and A3 opportunity is higher ($o = 2$) than that of Actors A1 and A4 ($o = 1$). For Scenarios S_7, S_8, S_9, and S_{10}, there is no time constraint, but there is still a space constraint. Scenarios S_7 and S_8 require the actor to be near either the patient's home or the hospital to access their network, whereas for Scenarios S_9 and S_{10} the actor must have physical access to the targeted devices. Similarly as for Scenario S_7, since the attack takes place near to the patient's home Actors A2 and A3 opportunity ($o = 3$) will be higher than the one of Actors A1 and A4 ($o = 2$). For Scenario S_8, however, all actors' opportunity score is the same ($o = 3$) since the attack takes place in a public site. In Scenarios S_9 and S_{10}, since the attack requires physical access to the device Actors A2 and A3 opportunity ($o = 2$) is higher than that of A1 and A4 ($o = 1$).

Motivation All actors benefit from the crime. They gain system information. Actor A2 motivation ($m = 4$) is the highest since the goal of this attack is the purpose of their profession. Actors A3 and A4 follow them with the same level of motivation ($m = 3$). The motivation of Actor A1 ($m = 2$) is the lowest because obtaining system information is not an end but a means to accomplish their activities.

4.3.3 Attack goal G3

Capacity Attack scenarios S_{11}, S_{12}, and S_{13} consist of introducing reading or calibration errors on the CIED's ecosystems devices. To do that, knowledge of the device's inner workings and advanced programming skills are required. Since there is some but not a lot of available information about how programmers and monitors work, in Scenarios S_{11} and S_{13} the capacity of Actor A1 ($c = 4$) will be higher than that of Actors A3, A4, and A5 ($c = 3$). The reason is that Actor A1 is an expert in the development of malicious code. On the other hand, there is much less information available about CIED and their architecture. Thus, for Scenario S_{12}, the capacity of the actors will be the same ($c = 2$). This is because while Actor A1 is an expert in malware development, Actors A3, A4, and A5 are more likely to obtain the CIED's mode of operation either by hiring personnel skilled in CIED programming or by using other illegal methods.

Opportunity For Scenarios S_{11} and S_{12}, there are constraints in terms of time and space. Scenario S_{11} takes place in the hospital during a session update. Scenario S_{12} must be performed near the patient and during incoming wireless communication with one of the externals devices. In these scenarios, we apply the same opportunity values that we have applied to the Scenarios S_6 and S_4 for Actors A1, A3, and A4. That is to say that in Scenarios S_{11} and S_{12}, Actor A3's opportunity ($o = 2$) is higher than that of Actors A1 and A4 ($o = 1$), we give to Actor A5 the same opportunity value as Actor A3 ($o = 2$) because we consider that a competent assassin for hire can have the same skills as a secret agent to sneak into public places without being noticed. On Scenario S_{13}, there is only a space restriction, and the same reasoning as in Scenario S_8 is applied: All actors have the same opportunity ($o = 3$).

Motivation All the actors (A1, A3, A4, and A5) benefit from the attack. Actors A1 and A5 conduct these attacks to make money, whereas Actors A3 and A4 are motivated by the opportunity to cause harm. Actor A5's motivation is high ($m = 4$) because not only will he earn a large amount of money but also each attack (succeeded) represents an opportunity to increase his reputation and therefore gain new clientele. Actors A3 and A4's motivation is the same ($m = 3$); although high, it is lower than that of Actor A5. Actor A1 is the one with the lowest motivation ($m = 1$) since for the latter there are other ways to make more money faster.

4.3.4 Attack goal G4

Capacity Actors' capacity is high on Scenarios $S_{11(a)}$ and $S_{11(c)}$ since there is extensive information about the external programmer behavior. Among all the actors, Actor A5 is the one with the most expertise in converting medical devices into weapons to kill. Thus, Actor A5's capacity ($c = 4$) is higher than that of Actors A3 and A4 ($c = 3$). For Scenario $S_{11(b)}$, knowledge of cardiology is required, and Actors A3 and A5 are more likely to have access to personnel with such knowledge or hiring it. Thus, Actors A3 and A5's capacity ($c = 2$) is higher than that of Actor A4 ($c = 1$). On Scenario S_{12}, the capacity of the Actors A3, A4, and A5 will be the same ($c = 2$). The reasoning is the same as that for Scenario S_{12} (Sect. 4.3.3), namely the lack of information concerning the CIED's behavior and implementation.

Opportunity In Scenario S_{12}, there are still constraints in terms of time and space. The actor must be close to the patient to send radio commands with its antenna to the CIED. Moreover, the attack must take place while the wireless communication is established in the CIED. As in the other scenarios where these constraints are present, the opportunity of Actors A3 and A5 ($o = 2$) is always higher than that of Actor A4 ($o = 1$). Besides, the analysis of the opportunity factor for Scenario S_{11} on Attack Goal G3 (Sect. 4.3.3) applies to Scenarios $S_{11(a)}$, $S_{11(b)}$, and $S_{11(c)}$. That is to say that the opportunity of Actors A3 and A5 ($o = 2$) is higher than that of Actor A4 ($o = 1$).

Motivation This attack goal aims at harming the health of an individual. Thus, it is Actor A3 ($m = 2$) and Actors A4 and A5 ($m = 3$) that benefit from this attack. We do not give them maximum motivation because there are faster and equally subtle ways to achieve this goal.

4.3.5 Attack goal G5

Capacity For Scenario S_{10}, the analysis is made in Sect. 4.3.2 in terms of capacity applies. It is the same with the Scenario S_{11} and the analysis in the Sect. 4.3.3. In Scenario S_{14}, a replay attack is performed. There is no major challenge in conducting this attack, which consists of periodically transmitting a wake-up command to the CIED employing an SDR. Thus, Actors A1, A3, and A4's capacity is the same ($c = 3$).

Opportunity The reasoning in Sects. 4.3.2 and 4.3.3 will apply to Scenario S_{11} and Scenario S_{14}, respectively. In Scenario S_{14}, there are constraints in terms of time and space, i.e., the opportunity of Actors A3 ($o = 2$) is higher than that of Actors A1 and A4 ($o = 1$).

Motivation In terms of motivation, the same reasoning than for Attack Goal G3 (Sect. 4.3.3) is applied.

5 Combined risk assessment

Risk assessment values range between 3 and 48. They are calculated as the probability (ranging from 3 to 12) multiplied by the impact (from 1 to 4). We calculate the risk separately for each impact category. This way of doing things gives insight of the risk that each threat (scenario, actor) represents separately for the health, economy, quality of life, and privacy impact categories. Consequently, this analysis responds to the needs of several different groups such as medical practitioners, regulators, manufacturers, and even patients. Each will know what the riskiest threat is for him and therefore the one to treat with priority. We ranked the risks in Table 6. Depending on the risk value, different risk management strategies can be chosen and applied. There are four strategies for managing risk, namely *refuse*, *accept*, *transfer*, or *manage* the risk. The most drastic is to refuse the risk, which is when the risk is considered unacceptable because of the catastrophic consequences it may have on the victims. In those cases, it is recommended to prohibit, stop using, or remove the system posing the threat. The strategy of accepting the risk is applied when the risk is either negligible or acceptable. That is to say when the benefits that the system brings outweigh its potential risks. Transferring the risk relies on giving risk management responsibility to a third party such as an insurance company. This is a strategy that does not apply to those threats where the impact is on patient health or quality of

Table 6 Risk characterization

Risk level	Values	Risk treatment
🟥 Unacceptable	$R > 127$	Refuse
🟧 Undesirable	$36 < R \leq 127$	Manage
🟨 Acceptable	$12 < R \leq 36$	Accept
🟩 Negligible	$0 \leq R \leq 12$	Accept

life. Finally, the risk mitigation or risk treatment consists in reducing the risk as much as possible with available means. This can be done through the updates of the systems, stricter regulations, or even awareness campaigns.

5.1 Results

The attacks goals of inducing medical staff to make errors (G3) and alter device behavior to endanger patient (G5) represent a risk for patient health. Those to gain knowledge of device operation and software (G2), induce medical staff to make errors (G3), disrupt or lower quality of patient follow-up (G4), and alter device behavior to endanger patient (G5) represent an economic risk to manufacturers and health organizations. We can then note that G3 and G5 represent a risk for all groups. In terms of privacy or degradation of life quality, none of the attack goals represent a potential risk that needs to be managed. In this section, we focus on those threats representing either an unacceptable or an undesirable risk for the victims' health and economy. The risk results of all the threats herein considered are found in Table 6 of A.

5.2 Discussion

5.2.1 Monetary risk assessment

5.2.1.1. Monetary risk assessment by attack goals
Attack goal G2 This attack goal represents a major risk in terms of economic losses. The victim can be either the manufacturer or the hospital. As hospitals are public organization, it can be considered that it is the whole society that is the victim. G2 contains five unacceptable threats (Scenarios S_4, S_5, S_6, S_7, S_8, and S_9 with all actors). These threats should be managed with high priority. By analyzing these threats, we can see that the actor's attack method is always the same, namely exploiting the authentication mechanisms of the target systems, i.e., the external devices and cloud-based systems with which they interact. This fact in itself is good news. On the one hand, external devices are not constrained by the resource limitations as the CIED are, so robust authentication solutions can be implemented without significant problems. There is a plethora of standard robust and proven solutions to secure system authentication, and there is no need to resort to proprietary, unproven solutions. We, therefore, propose the following solutions. The threats related to Scenario S_4 are solved by securing domestic networks. To do this, patients must take the habit of securing their networks with robust passwords, i.e., passwords with high entropy. The entropy is an indicator of how uncertain (random) an information source is. Thus, by using passwords with high entropy, the patients will be reducing the risk of being victims of brute-force attacks. There are tools available online to compute the entropy of information sources and that can help users generate high-entropy memorable passwords. Furthermore, the patient should pay attention to the other Internet of things (IoT) devices that are connected to his network, as they can be the entry door to their network. Accordingly, they should ensure that all devices in their networks are secured with a password.

To solve the threats associated with Scenario S_5, it is essential to insist that Web developers use good code practices and that the source code of Web pages be periodically reviewed.

To mitigate the threats associated with Scenario S_6, hospitals and manufacturers should adopt more reliable VPN solutions even if they require more investment. On top of that, their network should be equipped with prevention mechanisms such as the Early Warning System (EWS) presented in [48]. Besides, hospitals and manufacturers should consider recruiting cybersecurity professionals and technical services whose responsibility will be to ensure that there are no cybersecurity threats in their systems and/or networks, including those used for CIED programming and management.

For the threats associated with Scenarios S_7 and S_8, the solution involves securing USB ports of monitors and programmers with passwords with high entropy.

The threat posed by Scenario S_9 must be managed by ensuring the physical security of the target devices, in this case, programmers. Besides, it would be necessary to carry out awareness campaigns among the staff who use those devices, so that they become aware of the scope of the problem and therefore more attentive to the physical security of these devices.

The threat related to Scenario S_{10} represents an undesirable risk that can be reduced by using passwords with high entropy to protect the ports of the monitor's debugging interface.

Attack goal G3 The threats associated with the Scenarios S_{11} and S_{13} represent an undesirable risk. To mitigate the first threat, hospitals and manufacturers should adopt more reliable VPN solutions. The mitigation of the second threat involves securing the USB ports of the programmers using passwords with high entropy.

5.2.1.2. Monetary risk assessment by attack vectors From an economic point of view, the vulnerabilities V_6, V_7, V_9, and V_{15} must be eliminated, because their exploitation constitutes an unacceptable risk for the hospitals and the manufacturers. V_6 is eliminated by using good programming practices

Table 7 Results of the monetary risk assessment

Risk level	Treatment
🟥 Unacceptable	Refuse
🟧 Undesirable	Manage
🟨 Acceptable	Accept
🟩 Negligible	Accept

Attack goal	Scenario	Attack vector	P_{rMax}	I	R
G_1 Access patients sensitive data	S_1	3	7	1	7
	S_2	3	7	1	7
	S_3	10,13,14	6	1	6
	S_4	15	7	1	7
G_2 Gain Knowledge of device operation and software	S_4	15	9	4	36
	S_5	6	11	4	44
	S_6	7	9	4	36
	S_7	9	10	4	40
	S_8	9	10	4	40
	S_9	8	7	4	28
	S_{10}	10,11,12	5	4	20
G_3 Induce medical staff to make errors	S_{11}	7	8	3	24
	S_{12}	1,4,5	7	3	21
	S_{13}	9	9	3	27
G_4 Alter device behavior to endanger patient	$S_{11(a)}$	7	7	3	21
	$S_{11(b)}$	7	6	3	18
	$S_{11(c)}$	7	7	3	21
	S_{12}	1,4,5	6	3	18
G_5 Alter device behavior to decrease quality of life	S_{10}	10,11,12	7	2	14
	S_{11}	7	8	2	16
	S_{14}	2	8	2	16

and revising the source code of the programmers' software, and V_7 by securing hospital networks, and adopting more reliable VPN solutions. The security of hospital networks can also be improved by implementing efficient identity and access management (IAM) rules. For V_9, it is necessary to secure the USB ports of the external devices with robust passwords. Finally, securing home networks with robust passwords would eliminate the vulnerability V_{15}. Once the vulnerabilities mentioned above have been addressed, vulnerability V_8 must be managed as a priority because its exploitation constitutes an undesirable risk for hospitals. To do that, they must ensure the physical security of the programmer devices.

5.2.2 Health risk assessment

5.2.2.1. Health risk assessment by attack goals

Attack goal G3 The results of Table 8 reveal that G3 is the riskiest attack goal in terms of health. This is because of the unacceptable risk that Scenario S_{13} represents, i.e., the insertion of malware on the programmer through a USB port connection aimed to generate reading errors. Among the riskiest threats of this attack goal, this one must be managed with priority. However, the solution is simple: Use passwords with high entropy to protect USB port connection. During our observation of operations in a pacemaker clinic, we observed that it is common practice for staff to record the readings of the programmer (during follow-up sessions) in a USB key and then insert the key into a medical report formatting software in a separate computer system. We recommend that staff pay attention because this USB key could be the target of the actors. They could install the malware on it, and it would infect the programmer. Secondly, the computer where the software is located could also be the target of the actor. This means that the actor could infect the computer; subsequently, the computer would infect the USB key, and then the programmer. Thus, it is necessary to pay attention to who is using the USB key and then to ensure that the computer containing the report formatting software is itself secure (e.g., not connected to the network, unless strictly necessary).

The threats related to Attack Scenarios S_{11} and S_{12} constitute an undesirable risk that needs to be mitigated. For Scenario S_{11}, the threat consists of the insertion of malware into the programmer. S_{11} is achievable by accessing the device network during the programmer update session. The threat, as mentioned above, is avoidable by securing the health center network. Accordingly, it is necessary to implement an efficient method of identity and access management (IAM) of the computer systems of those entities. On the other hand, S_{12} threat takes advantage of the improper restriction of communication channels during the programmer updates. As mentioned in Sect. 4.1, those updates are achieved through a VPN between the device and the entity in charge of the updates. Thus, the health centers and manufacturers must invest in reliable solutions of VPN. For Scenario S_{12}, the threat is the insertion of malware on the CIED. This threat is due to the lack of robustness of the CIED authentication mechanisms. One potential solution consists in implementing more robust authentication mechanisms by using well-known techniques (e.g., asymmetric cryptography). However, CIED are limited in terms of computing resources and such solutions are not the most appropriate. There are, however, other more adequate solutions, which could be applied during the CIED manufacturing process. In particular, we propose that manufacturers use whitelisting techniques in the CIED software, which would prevent devices other than the programmer from sending commands to the CIED.

Attack goal G5 The successful completion of Scenarios $S_{11(a)}$ and $S_{11(c)}$ constitutes unacceptable risks, while that of $S_{11(b)}$ and S_{12} constitutes undesirable risks. As the attack Scenarios of G5 are the same as those of G3, the recommendations made for G3 therefore also apply here.

5.2.2.2. Health risk assessment by attack vectors From a health point of view, vulnerability V_9 must be eliminated because its exploitation represents an unacceptable risk to the health of individuals. This is feasible by securing the USB ports of the external devices with strong passwords. Once V_9 is adequately managed, Vulnerabilities V_6, V_7, and V_5 must be managed as a priority because their exploitation constitutes an undesirable risk. To mitigate the risk that V_6 represents, good programming practices and code source revision must take place on the programmer software. To reduce the risk associated with V_7, the hospital networks must be secured, and reliable VPN solutions must be applied. Finally, to mitigate V_5 it is necessary to apply whitelisting techniques on the CIED.

6 Related works

The Medical Device Privacy Consortium (MDPC) developed a framework [49] for assessing the cybersecurity risk of all types of medical devices. The authors used the NIST Special Publication 800-30 and FDA guidelines; they focused on assessing the impact on confidentiality, integrity, and availability of information. Alvarenga and Tanev presented a risk analysis method [50] that enriches the methodology proposed in [49] by integrating the blueprint approach of [51] and the value-sensitive design approach. This approach is based on the idea that the best design is the one that brings the most value to all stakeholders [52]. Indeed, it allows to identify which safety features add value for stakeholders and which ones are barriers for them. Coronado et al. implemented an Integrated Systems Management (ISM) program to assess the risk associated with electronically Protected Health Information (e-PHI) [53]. The risk assessment was conducted in the form of a questionnaire based on the NIST Special Publications 800-30 and 800-66 and the Health Insurance Portability and Accountability Act (HIPAA) regulations. As in the MDPC study [49], the assessment of this study focused on controls, policies, and procedures that affected the confidentiality, integrity, and availability of information in this case e-PHI. Wu and Eagles [54] proposed that cybersecurity risk analyses of medical devices should be based on safety analyses such as that of the ANSI/AAMI/ISO 14971 standard jointly developed by the American National Standards Institute (ANSI), the Association for the Advancement of Medical Instrumentation (AAMI), and the ISO. Through their work, the authors aimed to assist manufacturers when documenting their risk analysis to meet the premarket submission requirements. An improved version of the ANSI/AAMI/ISO 14971 standard was later proposed [55]. It specifies the process that manufacturers must follow to identify the hazards affecting medical devices, estimate and evaluate the risks to which they are exposed, control those risks, and monitor the effectiveness of the controls put in place.

Similar to previous works [49,50,53], our study is based on the recommendations of the NIST Special Publication 800-30, but unlike the proposition by Coronado et al. [53] which is not on the form of a questionnaire. In addition, we employ a threat-oriented analytical approach, while the MDPC [49] and the Alvarenga and Tanev work [50] used an impact-oriented method. This threat-oriented approach focuses on the attack (the attacker, his objectives, and the attack techniques he uses), while the impact-oriented approach concentrates on asset values and the impact on these assets [56]. Furthermore, our approach to assessing the impact of the attacks differs from those used in these previous studies [49,50,53,54]. In the MDPC [49] and Coronado et al. studies, the impact was assessed on confidentiality, integrity, and availability of information, while in this work we evaluate the impact of the attacks according to four separate aspects: health (H), monetary (M), privacy (P), and quality of life (QL). Thus, the outcomes of the risk assessment presented here may support the objectives of different kinds of organizations potentially interested in CIED risk assessment, e.g., health regulation agencies, device manufacturers, health practitioners, etc. Similarly to Wu and Eagles [54], we believe that risk analysis of medical devices must take into account the safety aspect. That is why we measure the impact on patient's health and quality of life. However, rather than assessing the impact on health according to classical safety standards as in [54], we use the Hayes classification [21], a reference in the fields of cardiology and electrophysiology. This impact classification is used to measure the degree of patient discomfort when the DECI do not function as expected due to external sources of magnetic interference

Table 8 Results of the health risk assessment

Risk level	Treatment
🟥 Unacceptable	Refuse
🟧 Undesirable	Manage
🟨 Acceptable	Accept
🟩 Negligible	Accept

Attack goal	Scenario	Attack vector	P_{rMax}	I	R
G_3 Induce medical staff to make errors	S_{11}	7	8	4	32
	S_{12}	1,4,5	7	4	28
	S_{13}	9	9	4	36
G_4 Disrupt or lower quality of patient follow-up	S_4	15	7	2	14
	S_{11}	7	7	2	14
	S_{12}	1,4,5	7	2	14
	S_{14}	2	7	2	14
	S_{15}	10	8	2	16
G_5 Alter device behavior to endanger patient	$S_{11(a)}$	7	7	4	28
	$S_{11(b)}$	7	6	4	24
	$S_{11(c)}$	7	7	4	28
	S_{12}	1,4,5	6	4	24

(e.g., an RF cyber-attack). We consider that such a classification captures the impact on patient health with more precision than that achievable with existing standards [55] that remain general in their approach.

Jagannathan and Sorini conducted a full IMD-specific cybersecurity risk analysis and presented their methodology [20]. The method was a traditional preliminary hazards analysis (PHA) study which was tailored to assess the cybersecurity properties of medical equipments. Rios and Butts [15] conducted an exhaustive analysis of the CIED ecosystem and the interdependence between its elements. The hardware and software components of different models of CIED, external programmers, and home-monitoring devices from different manufacturers were examined. As a result, over 8,000 known vulnerabilities were discovered in third-party libraries of four external programmer models belonging to four different manufacturers. In addition, vulnerabilities were found in all CIED evaluated. The publication of this work preceded the massive recall of CIED ordered by the FDA in August 2017, based on the vulnerabilities reported by ICS-CERT.

The Jagnnathan and Sorini study [20] analyzes the cybersecurity risk of fictitious medical devices. Thus, its findings do not reflect the actual state of the problem. In our work, we analyze real medical devices that are currently in the market. Therefore, the results herein find not only illustrate the actual scope of the problem but can serve as a basis for the risk management procedures related to the CIED ecosystem. Moreover, even though the Rios and Butts study [15] identifies the threats and their nature, the real scope of the risk that those threats entail is not described. We consider that although there are vulnerabilities in a system, it is their probability of exploitation and the impact that this exploitation has on individuals that determines whether the vulnerability represents a significant risk or not. In our study, we estimate the risk of a vulnerability based on the probability that it will be exploited and the impact that the exploitation will have on victims.

Tanev et al. conducted a cybersecurity risk assessment of networked medical devices [51]. The authors employed the value blueprint approach [57] used in the field of entrepreneurial innovation to help companies when implementing an ecosystem. Indeed, the author's purpose was to change the way manufacturers address cybersecurity during the device development process, i.e., make it something to be implemented during the process instead of something added at the end. Stine et al. [58] presented a cybersecurity risk assessment method for network-connected medical devices. This study introduced a scoring system relying on a cybersecurity questionnaire based on a model developed by Microsoft for classifying threats, namely the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) model. Their scoring system is intended to help healthcare organizations in identifying those medical devices that have the potential to endanger patient health or disrupt the quality of medical follow-up. Abrar et al. [59] conducted a risk analysis on cloud computing within the context of health applications, to evaluate their suitability for the Health Infrastructure System (HIS). The research team identified HIS vulnerabilities and then analyzed the impact that a security breach would have on its integrity if the vulnerable elements were deployed in a cloud computing environment. Stellios et al. presented a risk-based methodology to assess the criticality of IoT-enabled cyber-attacks [60]. This methodology applies to critical generic contexts, health environment is among them.

The scope of our study is broader than that of these four studies [51,58–60] in the sense that we also analyze unconnected devices such as the CIED itself. Stine et al. [58] estimated the probability of occurrence of an attack according to the security features implemented in the target system. Since the estimate of P is only based on the technical difficulty of the attacks, it does not adequately reflect reality. Just because an attack is technically simple to carry out does not mean that an attacker will be interested in achieving it. The chance and willingness to attack are essential factors when it comes to estimating P. Accordingly, in our study, we estimated P as a function not only of the characteristics of the target system but also as a function of specific characteristics of the attacker. Furthermore, Abrar et al. [59] analyze a mortgage situation (i.e., a fictional situation), while we analyze a real situation, i.e., the risk that current CIED cloud-based services represent for patient safety. Finally, Stellios et al. [60] conduct a generalized IoT risk analysis and does not take into account the specific characteristics (software, hardware) of the devices analyzed. Therefore, the study ignores through several risk factors. In our work, we focus on concrete devices (the CIED ecosystem) and analyze all of their characteristics. As a result, we can identify more potential threats.

7 Conclusion

As evidenced by previous work, CIED are vulnerable to cyber-attacks that use their RF interfaces to communicate with external devices (programmer and home monitor). This fact has been proven by the realization of radio attacks against the CIED RF communication interface in research laboratories [13,14]. Additionally, the telemetry functionality of the externals devices introduces vectors of cyber-attacks [15]. Although the vulnerabilities mentioned above exist, no attacks have been reported until now in real life, i.e., in an environment other than the controlled environment of research laboratories.

Thus, it remained to be determined how viable such an attack would be on an actual target (person or device) in the real world. This led us to the following research question: What are the real risks of cyber-attacks onto CIED and the systems they depend on (programmer, monitor, cloud-based systems)? To answer this question, we carried out a realistic risk analysis of such attacks, with regards to their impact at four scales: health, economy, quality of life, and privacy. We proceeded in this way because the problem under study affects many different groups, namely patients, practitioners, manufacturers, and more broadly states. Accordingly, separating the scales aims to individually support those groups' objectives in terms of risk management.

We did three kinds of analysis. First, an actor-based risk analysis to determine who the actors are and what their attack goals are. This analysis allowed us to determine the level of impact of the attacks. We then made a scenario-based risk analysis to determine the probability of occurrence of the attacks. Finally, we performed a combined risk analysis by considering the impact and probability results. We determined the most dangerous attack goals on the one hand and the most dangerous vulnerabilities on the other.

Our work reveals that the vulnerabilities associated with the RF communication interface of CIED represent an acceptable risk. This is due to the fact that these vulnerabilities have a low probability of being successfully exploited in real conditions (environment other than a research laboratory). However, the network and Internet connectivity of external devices represents a risk that in some cases is unacceptable, i.e., a risk that must be absolutely refused. The answer to our research question is therefore that the real risk is in the external devices and not in the CIED and that this risk is due to the increasing connectivity of said devices. We can therefore see that the problem under study is the medical variant of the trendy cybersecurity problem: the lack of security of connected objects (Internet of things or IoT).

Moreover, our analysis revealed that the attack goals (G2) *Gain knowledge of device operation and software* and (G3) *Induce medical staff to make errors* are the main attack goals of the actors. This result shows that while attacks on these devices affect patients, the patients are not always the target as we may have thought so far. The targets in many cases are manufacturers (intellectual property theft) and practitioners (threat of civil liability) for purely economic reasons. Manufacturers should, therefore, be aware of the problem and focus on the computer security of their equipment. The first step to this is avoiding secrecy regarding the software and architecture of their equipment. As has been often posited, code is more secure when it is open source since several people can test it and report errors so that they can be patched. This secrecy about code instead of protecting manufacturers exposes them more to cybersecurity risk. Health centers have to become more selective and demanding with the equipment they buy and implant on patients, as this would allow them to put more pressure on manufacturers to make the right cyber security choices.

8 Recommendations and future works

The outcomes of the risk analysis reveal that the higher risk factors correspond to network attacks or Web attacks against the external devices on which CIED depend. Accordingly, it is essential and a priority to strengthen the security of those devices, the networks in which they are deployed, and the cloud-based medical services that depend on them.

There exist countermeasures and solutions that can be set up instantly. Therefore, it is the responsibility of those operating these devices and services (including patients) to adopt the appropriate security measures. Also, it would be necessary that governments develop awareness campaigns and harden legislation as they do, for example, for driving safety or drug consumption. This legislation should address all parties by penalizing not only manufacturers but also hospitals and patients who neglect the security of those devices.

Besides, the results of this study show that the risk of an implanted CIED being attacked via the malicious exploitation of its RF communication interface is comparatively low. Consequently, a cybersecurity investment in CIED is not as high a priority as it is for external devices. The adoption of an immediate solution to counteract such threats without proper prior validation by the cybersecurity community could be inadequate, as it has often been the case in the past. Furthermore, securing the communication and authentication mechanisms of CIED has always been and continues to be a challenge. The limitations in terms of energy, memory, and computational capacity of these devices make it difficult to adopt traditional authentication and encryption used in other areas, such as Web security and other cyber-physical systems [61]. Alternative methods must be implemented. Some have already been proposed in previous works, namely those based on the biometric data of individuals [62–64], the proximity between devices [65], and the use of a proxy device [66,67] to perform authentication. However, none of these techniques satisfies the trade-off needed between the safety and the security of CIED. Therefore, to solve the threats affecting CIED, it is necessary to invest in the long term, i.e., to support and intensify research work while encouraging greater collaboration between researchers and the manufacturers of these devices. In the actor-based analysis, we did not consider accidental actors, i.e., people who could be a source of threat through negligence or inadvertence. Future work should include them in order to identify more threats (actor, scenario) and develop effective awareness campaigns. Furthermore, the vulnerabilities we have analyzed correspond to the CIED. However, there are vulnerabilities specific to other IMD [68,69]. Thus, we propose to extend this study to other IMD, such as insulin pumps, brain chips, and cochlear implants.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Appendix A: Risk assessment by attack goals and impact type

See Table 9.

Table 9 Risk assessment results

Risk level	Treatment
🟥 Unacceptable	Refuse
🟧 Undesirable	Manage
🟨 Acceptable	Accept
🟩 Negligible	Accept

				H		M		LQ		P	
Attack goal	Scenario	Attack vector	P_{rMax}	I	R	I	R	I	R	I	R
G_1	S_1	3	12	-	-	1	🟩 12	-	-	2	🟨 24
	S_2	3	12	-	-	1	🟩 12	-	-	2	🟨 24
	S_3	10,13,14	8	-	-	1	🟩 8	-	-	2	🟨 16
	S_4	15	12	-	-	1	🟩 12	-	-	2	🟨 24
G_2	S_4	15	32	-	-	4	🟥 128	-	-	-	-
	S_5	6	48	-	-	4	🟥 192	-	-	-	-
	S_6	7	32	-	-	4	🟥 128	-	-	-	-
	S_7	9	48	-	-	4	🟥 192	-	-	-	-
	S_8	9	48	-	-	4	🟥 192	-	-	-	-
	S_9	8	32	-	-	4	🟥 128	-	-	-	-
	S_{10}	10,11,12	16	-	-	4	🟧 64	-	-	-	-
G_3	S_{11}	7	24	4	🟧 96	3	🟧 72	1	🟨 24	-	-
	S_{12}	1,4,5	16	4	🟧 64	3	🟨 48	1	🟨 16	-	-
	S_{13}	9	36	4	🟥 144	3	🟧 108	1	🟨 36	-	-
G_4	S_4	15	12	2	🟨 24	3	🟨 36	1	🟩 12	-	-
	S_{11}	7	12	2	🟨 24	3	🟨 36	1	🟩 12	-	-
	S_{12}	1,4,5	12	2	🟨 24	3	🟨 36	1	🟩 12	-	-
	S_{14}	2	18	2	🟨 36	3	🟧 54	1	🟨 18	-	-
	S_{15}	10	18	2	🟨 36	3	🟧 54	1	🟨 18	-	-
G_5	$S_{11(a)}$	7	32	4	🟥 128	3	🟧 96	-	-	-	-
	$S_{11(b)}$	7	16	4	🟧 64	3	🟧 48	-	-	-	-
	$S_{11(c)}$	7	32	4	🟥 128	3	🟧 96	-	-	-	-
	S_{12}	1,4,5	16	4	🟧 64	3	🟧 48	-	-	-	-
G_6	S_{10}	10,11,12	12	-	-	2	🟨 24	2	🟨 24	-	-
	S_{11}	7	18	-	-	2	🟨 36	2	🟨 36	-	-
	S_{14}	2	18	-	-	2	🟨 36	2	🟨 36	-	-

Appendix B: Vulnerabilities

V_1: **Weak authentication algorithms**
Certain CIED use Time-based One-time Password (TOP) for authentication. The external devices authenticate to the CIED by computing a password from the current time and a shared secret, i.e., a secret cryptographic key shared between the CIED and both the external programmer and the home-monitoring device; for certain CIED, the secret key is their serial or model number. TOP authentication algorithms are vulnerable to identity theft attacks since an adversary who steals the secret key can generate valid passwords every time he wants to establish a telemetry session with the device [13,25,27,70,71].

V_2: **Boundless telemetry session duration**
The number of RF wake-up commands that a CIED can receive per session is not limited, i.e., an attacker can maintain a telemetry session indefinitely active by regularly sending the aforementioned commands to prematurely reduce the CIED's lifetime [14,23,25,28].

V_3: **Unencrypted data storage and transmission**
Certain CIED models store and transmit patient information without encrypting it. Thus, a nearby attacker may intercept the data exchanged between the CIED and the programmer or even gain access to the sensitive data stored on the device by sending an unauthorized RF command [13,25,29,70].

V_4: **Lack of command whitelisting techniques**
Command whitelisting is a computer protection method based on software restriction policy rules. This technique blocks by default the execution of all the pro-

grams contained in the device so that only programs that are the subject of a policy rule can be executed. In the case of CIED, there are no policy rules prohibiting the execution of programming commands from devices other than external programmers. Consequently, an adversary could send a programming command to the CIED by means of commercial available equipment such as a commercially available SDR [13,14,70].

V_5: **Unencrypted hardcoded authentication credentials**
The product username and password are stored in a recoverable format, i.e., without being previously encrypted [24,30].

V_6: **Software directory path traversal**
It has been shown that the software of certain devices contains directory path traversal vulnerabilities, i.e., a kind of software implementation vulnerability that permits the access to directories other than those permitted by design. Thus, an adversary will be able to exploit these weaknesses in order to read the external programmer's file system [24,31].

V_7: **Improper Restriction of Communication Channel**
Downloading software updates is done by means of a virtual private network (VPN) established between the programmer and its software update provider. While the use of VPN is a recognized good practice to secure communications between two parties, it has been unveiled that certain external programmers models do not verify that they are still connected to the VPN before the update operation is accomplished. Thus, an adversary could leverage the device's local network access features to interfere with the communication between the programmer and its software update provider [15,24,32].

V_8: **Exploiting embedded debugging interfaces (JTAG and UART)**
Embedded debugging interfaces are connection ports present in a device's printed circuits. Manufacturers use them to perform functional testing and redesign of devices after manufacturing. For example, JTAG is a master/server interface used to verify a circuit, test device logic, and perform functional redesign when needed. It can be used to read and modify the memory and the registers as well as to read the device's firmware. The UART interface provides a serial communication between the device's embedded systems and an external PC, i.e., a bidirectional interface used to send and receive data asynchronously. Since these interfaces allow direct access to the device memory and firmware, unprotected access to those interfaces constitutes an entry point for attacks against the CIED [15]. Home monitoring devices also have this vulnerability.

V_9: **Unprotected USB serial port connections**
Certain devices have USB port connections. They are frequently used by medical staff to store the information on a USB stick in order to transfer it to other systems, e.g., reporting software. If the USB port connection is not blocked with a password or another authentication mechanism, an attacker could connect to it and access data on the device and potentially take control of it [15].

V_{10}: **Unprotected removable media/hard drives**
When they are in the attacker's hands, the media/hard drives become an entry point of attacks since they can be used to extract information from a device's file system [15].

V_{11}: **OS Hardcoded authentication credentials**
In certain products, authentication credentials to the operating system (OS) are hardcoded on the device. That means that an adversary with physical access to the device's integrated circuit can access the OS by connecting to the debug port and authenticate with the hardcoded password [15,26,33].

V_{12}: **Exposed dangerous methods or functions**
Home monitors contain debug code to test their communication interfaces with both the CIED or the external system (databases, servers) of the cloud-based application used by the physicians. Thus, by leveraging this vulnerability an adversary with physical access to the monitor can maliciously exploit the debug code to accomplish a set of attacks, for example, read or write the device's memory content, interrupt the data sending to the cloud-based systems, and enable bidirectional communication with CIED [26,34].

V_{13}: **Server hardcoded authentication credentials**
The credentials that home monitors use to authenticate to the cloud-based systems supporting the patient's remote follow-up service are hardcoded on certain devices. Thus, an attacker with physical access to the monitor can leverage these vulnerabilities to access the database in order to read or tamper with the patient's medical data [15].

V_{14}: **Server hardcoded parameters**
In certain home monitors, the IP address of the authentication servers is hardcoded. An adversary could use this information to conduct a DoS attack to make the server temporarily unavailable by sending several Web requests to this IP address [15].

V_{15}: **Exploiting remote firmware update**
Firmware updates for home monitors are triggered remotely. Indeed, when the time comes to update the device's firmware, the manufacturer sends the new version to the monitor through the cloud. This method is advantageous from the patient's point of view since it avoids an additional trip to the hospital. However, it

constitutes at the same time an attack vector because the home-monitoring device does not verify the identity of the system distributing the firmware. An attacker could take advantage of this lack of verification by achieving a man-in-the-middle attack with the purpose of sending a counterfeit firmware to the device [15].

Appendix C: Sequence of events of the attack scenarios

S_1: Radio attack on the CIED-Programmer wireless communications.
(e_1) Acquire the hardware (SDR, antenna, signal processing software)
(e_2) Go to the hospital
(e_3) Be located at a distance relatively close to the CIED
(e_4) Configure the SDR in reception mode
(e_5) Perform a frequency scan of the MICS band to determine the transmission frequency of the CIED
(e_6) Intercept and record the signal transmitted by the CIED
(e_7) Read the patient's health data (V_3)
S_2: Radio attack on the CIED-Monitor wireless communications.
(e_1) Acquire the hardware (SDR, antenna, signal processing software).
(e_2) Go to the patient's home
(e_3) Be located at a distance relatively close to the CIED
(e_4) Configure the SDR in reception mode
(e_5) Perform a frequency scan of the MICS band to determine the transmission frequency of the CIED
(e_6) Intercept and record the signal transmitted by the CIED
(e_7) Read the patient's health data (V_3)
S_3: Unauthorized physical access to the monitor content
——————Using the JTAG interface———-
(e_1) Acquire the hardware (F to F jumper wire, in-debugger-circuits, PC with IDLE debugger)
(e_1) Go to the patient's home
(e_2) Take the patient's monitor
(e_3) Connect one extremity of the F to F jumper wire to the monitor debug port (exploiting V_{10})
(e_4) Connect the other extremity of the F to F jumper wire to the in-debugger-circuits
(e_5) Connect the in-debugger-circuit to the PC
(e_6) Access the monitor memory by means of the IDLE debugger
(e_7) Use V_{13} and V_{14} to adjust the server settings and credentials to authenticate to them
(e_8) Access the server by means of the information obtained in (e_8)
(e_9) Read the patient's medical data
——————Using the UART interface———-
(e_1) Acquire the hardware (Pirate bus, PC with IDLE debugger)
(e_2) Go to the patient's home
(e_3) Take the patient's monitor
(e_4) Connect one end of the pirate bus to the monitor debug port (exploiting V_{10})
(e_5) Connect the other pirate bus end to the PC containing the IDLE debugger
(e_6) Access the monitor memory by means of the IDLE debugger
(e_7) Use V_{13} and V_{14} to adjust the server settings and credentials to authenticate to them
(e_8) Access the server by means of the information obtained in (e_7)
(e_9) Read the patient's medical data
S_4: Network attack on the Monitor
(e_1) Gain access to the patient's router the day of the monitor's update
(e_2) Intercept the updated firmware (V_{15})
(e_3) Replace the firmware with a backdoor
S_5: Web attack on programmers' SW deployment network server
(e_1) Find the URL in which the programmer (app) retrieves files from the server
(e_2) Modify URL with commands and Web server escape code
(e_3) Send the URL to the server(via http request) (e_3)
(e_4) Extract the desired files
S_6: Network attack on the programmer's
(e_1) Go to the hospital the day of the update
(e_2) Access the programmer's network
(e_3) Leverage V_7 to gain access to the programmer
(e_3) Extract the desired files
S_7: Network attack on the Monitor
(e_1) Go to the patient home
(e_2) Access the patient network
(e_3) Access the monitor's USB port (V_9)
(e_4) Navigate in the file system and extract the desired files
S_8: Network attack on the programmer
(e_1) Go to the hospital
(e_2) Access the hospital network
(e_3) Access the monitor's USB port (V_9)
(e_4) Navigate the file system and extract the desired files
S_9: Physical attack on the programmer
(e_1) Go to the hospital
(e_2) Extract the programmer's removable hard drive(V_8)
S_{10}: Physical attack on the monitor
——————Using the JTAG interface———-
(e_1) Acquire the hardware (F to F jumper wire, in-debugger-circuits, PC with IDLEs debugger)
(e_2) Go to the patient's home
(e_3) Take the patient's monitor

(e_4) Connect one end of the F to F jumper wire to the monitor debug port (V_{10})
(e_5) Connect the other end of the F to F jumper wire to the in-debugger-circuits
(e_6) Connect the in-debugger-circuit to the PC
(e_7) Access the monitor memory by means of the IDLE debugger
(e_8) Use V_{11} and V_{12} to acquire the credentials of OS
(e_9) Access the OS of the monitor by means of the information obtained in e_8
(e_{10}) Read the OS
——————Using the UART interface———-
(e_1) Acquire the hardware (Pirate bus, PC with IDLE debugger)
(e_2) Go to the patient's home
(e_3) Take the patient's monitor
(e_4) Connect one end of the pirate bus to the monitor debug port (V10)
(e_5) Connect the other pirate bus end to the PC containing the IDLE debugger.
(e_6) Access the monitor memory by means of the IDLE debugger
(e_7) Use V_{11} and V_{12} to acquire the credentials of the OS
(e_8) Access the OS of the monitor by means of the information obtained in e_7
(e_9) Read information about OS
S_{11}: Network attack on the programmer
(e_1) Gain access to the CIED room consultation the day of the update
(e_2) Intercept the updated firmware (V_7)
(e_3) Replacing the firmware with malware
S_{12}: Radio attack on the CIED
(e_1) Acquire the hardware (SDR, antenna, signal processing software)
(e_2) Go to the hospital
(e_3) Be located at a distance relatively close to the CIED
(e_4) Configure the SDR in transmission mode
(e_5) Perform a frequency scan of the MICS band to determine the Programmer's transmission frequency
(e_6) Transmit commands (via RF signals) to the CIED (V_1,V_4,V_5)
S_{13}: Network attack on the programmer
(e_1) Go to the hospital
(e_2) Access the hospital network
(e_3) Access the monitor's USB port(V_9)
(e_4) Insert a malware
S_{14}: Radio attack on the CIED
(e_1) Acquire the hardware (SDR, antenna, signal processing software)
(e_2) Go to the hospital
(e_3) Be located at a distance relatively close to the CIED
(e_4) Configure the SDR in Transmission mode
(e_5) Perform a frequency scan of the MICS band to determine the programmer's transmission frequency
(e_6) Transmit wake-up commands (via RF signals) to the CIED periodically (V_1,V_2,V_4)

References

1. Cuvillier, E.: Handbook of Leads for Pacing. Defibrillation and Cardiac Resynchronization, Cardiotext (2011)
2. Savci, H.S., Sula, A., Wang, Z., Dogan, N.S., Arvas, E.: Mics transceivers: regulatory standards and applications [medical implant communications service]. In: Proceedings. IEEE SoutheastCon, pp. 179–182. IEEE (2005)
3. Sanders, R.S., Lee, M.T.: Implantable pacemakers. Proc. IEEE **84**, 480–486 (1996)
4. Biotronik USA: Eluna HF-T technical manual. https://manualzz.com/doc/7597543/eluna-hf-t---biotronik-usa (2015)
5. Medtronic: Medtronic carelink 2090 reference manual programmer for medtronic and vitatron devices. https://www.manualslib.com/manual/1410977/Medtronic-Carelink-2090.html#manual (2001)
6. Slotwiner, D., Varma, N., Akar, J.G., Annas, G., Beardsall, M., Fogel, R.I., Galizio, N.O., Glotzer, T.V., Leahy, R.A., Love, C.J., et al.: Hrs expert consensus statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. Heart Rhythm **12**, 69–100 (2015)
7. Ricci, R.P., Morichelli, L., D'onofrio, A., Calò, L., Vaccari, D., Zanotto, G., Curnis, A., Buja, G., Rovai, N., Gargaro, A.: Effectiveness of remote monitoring of CIEDs in detection and treatment of clinical and device-related cardiovascular events in daily practice: the homeguide registry. Europace **15**, 970–977 (2013)
8. Staylor, A.: New pacemakers. ICDs with home monitoring save time. Medscape Internal Medicine, LLC (2002)
9. Islam, M.N., Yuce, M.R.: Review of medical implant communication system (MICS) band and network. ICT Express **2**, 188–194 (2016)
10. FCC, et al.: Medical implant communications service (MICS) federal register. Rules Reg **64**, 69926–69934 (1999)
11. FCC: Regulations, MICS Band Plan, Table of Frequency Allocations, Part 95 (2003)
12. Bashirullah, R.: Wireless implants. IEEE Microwave Mag. **11**, 14–23 (2010)
13. Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W.H.: Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: IEEE Symposium on Security and Privacy (SP), pp. 129–142. IEEE (2008)
14. Marin, E., Singelée, D., Garcia, F.D., Chothia, T., Willems, R., Preneel, B.: On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In: Proceedings of the 32nd Annual Conference on Computer Security Applications, pp. 226–236. ACM (2016)
15. Rios, B., Butts, J.: Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies (2017)
16. Burns, A., Johnson, M.E., Honeyman, P.: A brief chronology of medical device security. Commun. ACM **59**, 66–72 (2016)
17. Food and Drug Administration: Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers: FDA safety communication. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (2017)

18. ISO/IEC: International Standard ISO/IEC 27005:2018, Information technology Security techniques Information security risk management (2018)
19. Ross, R.S.: NIST Special Publication 800-30 Rev. 1, Guide for Conducting Risk Assessments (2012)
20. Jagannathan, S., Sorini, A.: A cybersecurity risk analysis methodology for medical devices. In: 2015 IEEE Symposium on Product Compliance Engineering (ISPCE), pp. 1–6. IEEE
21. Hayes, D.L., Wang, P.J., Reynolds, D.W., Estes, N.M., Griffith, J.L., Steffens, R.A., Carlo, G.L., Findlay, G.K., Johnson, C.M.: Interference with cardiac pacemakers by cellular telephones. N. Engl. J. Med. **336**, 1473–1479 (1997)
22. NIST, FIPS 199, standards for security categorization of federal information and information systems (2004)
23. Hei, X., Du, X., Wu, J., Hu, F.: Defending resource depletion attacks on implantable medical devices. In: 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), pp. 1–5. IEEE (2010)
24. ICS-CERT: Advisory ICSMA-18-058-01 medtronic 2090 carelink programmer vulnerabilities (update b). https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-01 (2018)
25. ICS-CERT: Advisory ICSMA-17-241-01 Abbott laboratories accent/anthem, accent MRI, assurity/allure, and assurity MRI pacemaker vulnerabilities. https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01 (2017)
26. ICS-CERT: Advisory ICSMA-18-179-01 Medtronic MyCareLink Patient Monitor. https://ics-cert.us-cert.gov/advisories/ICSMA-18-179-01 (2018)
27. NIST, NVD-CVE-2017-12712 detail. https://nvd.nist.gov/vuln/detail/CVE-2017-12712 (2018)
28. NIST, NVD-CVE-2017-12714 detail. https://nvd.nist.gov/vuln/detail/CVE-2017-12714 (2018)
29. NIST, NVD-CVE-2017-12716 detail. https://nvd.nist.gov/vuln/detail/CVE-2017-12716 (2018)
30. NIST, NVD-CVE-2018-5446 detail. https://nvd.nist.gov/vuln/detail/CVE-2018-5446 (2018d)
31. NIST, NVD-CVE-2018-5448 detail. https://nvd.nist.gov/vuln/detail/CVE-2018-5448 (2018e)
32. NIST, NVD-CVE-2018-10596 detail. https://nvd.nist.gov/vuln/detail/CVE-2018-10596 (2018f)
33. NIST, NVD-CVE-2018-8870 detail. https://nvd.nist.gov/vuln/detail/CVE-2018-8870 (2018g)
34. NIST, NVD-CVE-2018-8868 detail. https://nvd.nist.gov/vuln/detail/CVE-2018-8868 (2018h)
35. ICS-CERT: Cyber threat source descriptions. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#gao (2005)
36. Piggin, R.: Cybersecurity of medical devices: addressing patient safety and the security of patient health information. BSI Group, Macquarie Park, Australia, White Paper (2017)
37. Cyberpolicy: Why medical records are 10 times more valuable than credit card info. https://cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit/-card-info (2018)
38. Sulleyman, A.: NHS cyber attack: why stolen medical information is so much more valuable than financial data. https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable/-to-sell-financial-a7733171.html (2017)
39. Lord, R.: The real threat of identity theft is in your medical records, not credit cards. https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records/-not-credit-cards/#12b202291b59 (2017)
40. Yao, M.: Your electronic medical records could be worth $ 1000 to hackers. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/ (2017)
41. Lucintel: Medical device market report: trends, forecast and competitive analysis. https://www.businesswire.com/news/home/20180423006381/en/Global-Medical-Device-Market-Report-2018-2023-Trends (2018)
42. Lind, K.D.: Understanding the market for implantable medical devices. Insight (2017)
43. Halligan, A.: The importance of values in healthcare. J. R. Soc. Med. **101**, 480–481 (2008)
44. Pilgrim, D., Tomasini, F., Vassilev, I.: Examining Trust in Healthcare: A Multidisciplinary Perspective. Macmillan International Higher Education (2010)
45. Van der Schee, E., Groenewegen, P.P., Friele, R.D.: Public trust in health care: a performance indicator? J. Health Organ. Manag. **20**, 468–476 (2006)
46. de Zulueta, P.: Truth, trust and the doctor–patient relationship. In: Primary Care Ethics, pp. 1–24. CRC Press (2018)
47. Cazorla, L., Alcaraz, C., Lopez, J.: Cyber stealth attacks in critical information infrastructures. IEEE Syst. J. **12**, 1778–1792 (2018)
48. Alcaraz, C., Fernandez-Gago, C., Lopez, J.: An early warning system based on reputation for energy control systems. IEEE Trans. Smart Grid **2**, 827–834 (2011)
49. MDPC: Security risk assessment framework for medical devices a Medical Device Privacy Consortium white paper (MDPC). Medical Device Privacy Consortium (MDPC), pp. 1–23 (2014)
50. Alvarenga, A., Tanev, G.: A cybersecurity risk assessment framework that integrates value-sensitive design. Technol. Innov. Manag. Rev. **7**, 32 (2017)
51. Tanev, G., Tzolov, P., Apiafi, R.: A value blueprint approach to cybersecurity in networked medical devices. Technol. Innov. Manag. Rev. **5**, 17–25 (2015)
52. Denning, T., Kramer, D.B., Friedman, B., Reynolds, M.R., Gill, B., Kohno, T.: CPS: Beyond usability: applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices. In: Proceedings of the 30th Annual Computer Security Applications Conference, pp. 426–435 (2014)
53. Coronado, A.J., Wong, T.L.: Healthcare cybersecurity risk management: keys to an effective plan. Biomed. Instrum. Technol. **48**, 26–30 (2014)
54. Wu, F., Eagles, S.: Cybersecurity for medical device manufacturers: ensuring safety and functionality. Biomed. Instrum. Technol. **50**, 23–34 (2016)
55. ANSI/AAMI/ISO: Medical devices application of risk management to medical devices (2019)
56. Aksu, M.U., Dilek, M.H., Tatli, E.I., Bicakci, K., Dirik, H.I., Demirezen, M.U., Aykir, T.: A quantitative CVSS-based cyber security risk assessment methodology for it systems. In: 2017 International Carnahan Conference on Security Technology (ICCST), pp. 1–8. IEEE
57. Adner, R.: The Wide Lens: A New Strategy for Innovation. Penguin, London (2012)
58. Stine, I., Rice, M., Dunlap, S., Pecarina, J.: A cyber risk scoring system for medical devices. Int. J. Crit. Infrastruct. Prot. **19**, 32–46 (2017)
59. Abrar, H., Hussain, S.J., Chaudhry, J., Saleem, K., Orgun, M.A., Al-Muhtadi, J., Valli, C.: Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access **6**, 19140–19150 (2018)
60. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. **20**, 3453–3495 (2018)
61. Camara, C., Peris-Lopez, P., Tapiador, J.E.: Security and privacy issues in implantable medical devices: a comprehensive survey. J. Biomed. Inform. **55**, 272–289 (2015)
62. Rostami, M., Juels, A., Koushanfar, F.: Heart-to-heart (h2h): authentication for implanted medical devices. In: Proceedings of

the 2013 ACM SIGSAC conference on Computer & communications security, pp. 1099–1112. ACM (2013)

63. Zheng, G., Fang, G., Shankaran, R., Orgun, M.A., Dutkiewicz, E.: An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices. In: International Symposium on Wireless Personal Multimedia Communications (WPMC), pp. 624–628. IEEE (2014)
64. Hei, X., Du, X.: Biometric-based two-level secure access control for implantable medical devices during emergencies. In: 2011 Proceedings IEEE INFOCOM, pp. 346–350. IEEE (2011)
65. Rasmussen, K.B., Castelluccia, C., Heydt-Benjamin, T.S., Capkun, S.: Proximity-based access control for implantable medical devices. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 410–419. ACM
66. Xu, F., Qin, Z., Tan, C.C., Wang, B., Li, Q.: Imdguard: securing implantable medical devices with the external wearable guardian. In: 2011 Proceedings IEEE INFOCOM, pp. 1862–1870. IEEE (2011)
67. Nesheim, T.A.: The BLE Cloaker: securing implantable medical device communication over bluetooth low energy links (2015)
68. Khera, M.: Think like a hacker: insights on the latest attack vectors (and security controls) for medical device applications. J. Diabetes Sci. Technol. **11**, 207–212 (2017)
69. NIST: NVD-CVE-2018-16986 detail (2018)
70. Breakpoint: BREAKPOINT 2012. http://2012.ruxconbreakpoint.com/ (2012)
71. Barnaby Jack, Pacemaker Hack can deliver deadly 830-volt joltl, http://white-hackers.blogspot.com/2012/10/pacemaker-hack-can-deliver-deadly-830.html (2012)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.