پزشکی همراه

حملات هکری به بدن بیماران

کارشناسان امنیتی هشدار داده‌اند، بسیاری از دستگاه‌های پزشکی تولیدشده توسط شرکت مِدترونیک در مقابل حملات سایبری آسیب‌پذیر هستند. ۱۷ مدل از دستگاه‌های تنظیم ضربان قابل‌نصب در بدن و تجهیزاتی که از خارج با آن‌ها ارتباط برقرارمی‌کنند در برابر این آسیب‌پذیری‌ها ضعیف هستند.

سخنگوی این شرکت مدعی است که این موارد آسیب‌پذیری توسط خود شرکت اطلاع‌رسانی شده و رخنه امنیتی یا حمله‌ای سایبری در کار نبوده است. خطر اصلی متوجه مدل‌هایی از دستگاه‌های تنظیم ضربان قلب موسوم به CRT-D و ICD است. کامپیوترها قادرند، خارج از بدن بیمار این دستگاه‌ها را برنامه‌ریزی کرده و اطلاعات آن‌ها را دریافت کنند. این دستگاه‌ها فرکانس‌های رادیویی منتشر می‌کنند که رمزگذاری نشده‌اند و می‌توان از فاصله چندمتری بدن، آن‌ها را شناسایی کرد. بر اساس هشدار کارشناسان امنیتی، یک فرد مهاجم می‌تواند با دسترسی به این سیگنال‌ها آن‌ها را مختل کند، تغییر دهد یا شنود کند.

محققان بیش از یک دهه است به‌طور مکرر هشدار می‌دهند، دستگاه‌های پزشکی در صورت سوءاستفاده می‌توانند به سلاح‌هایی کشنده تبدیل شوند. کارشناسان بارها نشان داده‌اند که چگونه می‌توان یک پمپ انسولین، ضربان‌ساز یا حتی کل شبکه یک بیمارستان را هک کرد. شرکت مدترونیک یکی از چندین شرکتی است که طی چند سال گذشته آسیب‌پذیری محصولاتش در برابر نفوذ هکرها به‌طور علنی اعلام شده است.
این شرکت‌ها همواره با بیان این‌که تاکنون به‌واسطه چنین حملاتی جان کسی به خطر نیفتاده، از پاسخگویی به انتقادات سر باز می‌زنند. یکی از مهندسان برق دانشگاه پُردو معتقد است: «رمزگذاری سیگنال‌های این دستگاه‌ها برای جلوگیری از نفوذ، کافی نیست.» محققان این دانشگاه مچ‌بندی طراحی کرده‌اند که انتشار امواج دستگاه‌های کارگذاشته شده در بدن بیمار را با استفاده از خصوصیات رسانایی بدن محدود می‌کند. به‌این‌ترتیب به‌عنوان‌مثال، سیگنال‌های تولیدشده توسط ضربان‌ساز، امکان گذر از پوست بدن را نخواهند یافت و درون بدن به دام می‌افتند. با این راهکار امکان دستیابی به سیگنال‌ها نیست، مگر این‌که ارتباط فیزیکی با بدن بیمار برقرار شود. این روش هنوز روی بیمارانی که دستگاه‌های پزشکی در بدنشان کار گذاشته‌شده، آزموده نشده است.

تاریخ انتشار:

24 تیر 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15706/%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D9%87%DA%A9%D8%B1%DB%8C-%D8%A8%D9%87-%D8%A8%D8%AF%D9%86-%D8%A8%DB%8C%D9%85%D8%A7%D8%B1%D8%A7%D9%86