FDA waarschuwt voor hackable implanteerbare hartproducten

12 januari 2017

Verander je hartslag

Hackers kunnen van afstand toegang krijgen tot iemands geïmplanteerd hartapparaat, waarmee ze de mogelijkheid hebben om de hartslag te wijzigen, schokken kunnen toedienen of de accu leeg kunnen laten lopen. Er zijn tot nu toe geen ongelukken gemeld met betrekking tot hacken, aldus de FDA. implanteerbare hartproducten van St. Jude Medical worden onder de huid geplaatst, in de borstkas en hebben geïsoleerde draden die in het hart geplaatst worden om het hart goed te laten kloppen.

De apparatuur is verbonden met de Merlin@home Transmitter, die zich in het huis van de patiënt bevindt. De zender stuurt gegevens van de patiënt naar hun arts met behulp van het Merlin.net Patient Care Network. Hackers kunnen toegang krijgen tot de zender, zo bevestigt de fabrikant. "Het kan worden gebruikt om geprogrammeerde opdrachten naar het geïmplanteerde apparaat te wijzigen," zo schrijft de FDA.

Een een vertegenwoordiger van St. Jude Medical verklaart in een e-mail dat het bedrijf “maatregelen heeft getroffen om de beveiliging en de veiligheid van onze toestellen te beschermen, inclusief de nieuwe software en een medische cybersecurity adviesraad heeft opgericht." Het bedrijf is van plan om nog meer updates uit te voeren in 2017, aldus de e-mail.

De waarschuwing van de FDA kwam een paar dagen nadat Abbott Laboratories de overname van St. Jude Medical had afgerond. Vier maanden eerder, in augustus 2016, publiceerde een groep deskundigen van het in Miami gevestigde cyber security bedrijf MedSec Holding een document waarin ze uitleggen dat ze verschillende problemen vonden in de pacemakers en defibrillators van St. Jude Medical. Deze publicatie werd gemaakt in samenwerking met het beleggingshuis Muddy Waters Capital.

Deuren open laten

"Merlin@huizen mist zelfs de meest basale vormen van security," zo is te lezen in de publicatie. De experts van MedSec schreven ook: "De belangrijkste kwetsbaarheden kunnen blijkbaar worden uitgebuit door een low level hackers. Vreemd genoeg heeft STJ letterlijk honderdduizenden deuren open gelaten in de vorm van de thuistransmitter (de zogenaamde "Merlin@home") die naar onze mening het ecosysteem van de STJ enorm openstellen voor aanvallen. Deze units gewoon te koop op Ebay, voor nog geen 35 dollar."

In augustus ontkende St. Jude Medical de claims nog en klaagden Muddy Waters en MedSec aan. “De aantijgingen zijn absoluut onwaar,” zo zei CTO Phil Ebeling tegen Bloomberg. “Er zijn diverse lagen in de beveiliging aangebracht. We voeren continu security assesments uit en we werken met externe deskundigen die zich specifiek op Merlin@home en op al onze toestellen focussen." St. Jude weigerde commentaar te geven over de lopende rechtszaken.

Muddy Waters is niet blij met deze update. Volgens hen is St. Jude Medical meer geïnteresseerd in winst dan in patiënten. "De aangekondigde oplossingen lijken de grotere

problemen niet echt aan te pakken, zoals het bestaan van een universele code waardoor hackers de implantaten kunnen overnemen," staat in een persverklaring. "Als we niet openbaar waren gegaan, had St. Jude de kwetsbaarheden niet opgelost."

Patch download automatisch

De onlangs vrijgegeven softwarepatch die de problemen moet oplossen is beschikbaar en zal automatisch downloaden naar de transmitter. "Patiënten moeten ervoor zorgen dat hun Merlin@home apparaat is aangesloten op het net en op een vaste of mobiele adapter, zodat ze deze en eventuele toekomstige automatische beveiligingsupdates kunnen ontvangen," valt te lezen in een persbericht van St. Jude Medical.

Dit is niet de eerste keer dat artsen en cybersecurity experts hun zorgen over geïmplanteerde medische apparaten hebben uitgesproken. Op 6 oktober publiceerde ICT & Health een artikel over een insulinepomp van Johnson & Johnson die gemakkelijk kon worden gehackt. De voormalige vicepresident van de VS Dick Cheney schakelde de wireless opties van zijn hartimplantaat een paar jaar geleden uit, uit angst voor een aanslag op zijn leven.