Task Force “Avarie e Complicanze”

Raccomandazioni AIAC relative all’avviso di sicurezza inerente il sistema di connessione wireless di un sottogruppo di dispositivi ICD e CRTD della ditta Medtronic

In data 21 marzo 2019 la ditta Medtronic ha comunicato un avviso di sicurezza inerente il sistema di connessione wireless utilizzato in un gruppo di dispositivi (ICD e CRTD) prodotti e commercializzati negli ultimi anni. Il problema è inerente al protocollo di trasmissione dati utilizzato per le funzioni telemetriche, il quale non garantirebbe una assoluta cybersicurezza e risulterebbe suscettibile di intromissione ed interferenza da operatori diversi da quelli sanitari.

I modelli interessati dalla segnalazione sono:
Amplia CRTD, Claria CRTD, Compia CRTD Concerto CRTD, Consulta CRTD, Evera ed Evera MRI ICD, Maximo II CRTD e ICD, Mirro ICD, Nayamed ND ICD, Primo MRI ICD, Protecta CRTD e ICD, Secura ICD, Virtuoso e Virtuoso II ICD, Visia AF ed MRI ICD, Viva CRTD.
Il sistema è usato dai **programmatori 2090** e **Carelink 24950**, **24952** e **2490C**.

Dati Tecnici

Un gruppo di esperti esterni alla Medtronic ha accertato che il protocollo di trasmissione dei dati wireless mediante RF denominato “Conexus” utilizzato nei modelli sopraelencati presenta delle lacune di cybersicurezza non possedendo un sistema di encriptazione, autenticazione o autorizzazione in grado di renderlo sicuro contro possibili tentativi di intromissione di soggetti esterni per l’accesso ai dati ed alla loro modifica.
Il sistema di telemetria in questione viene utilizzato dai sanitari per l’interrogazione del dispositivo e la programmazione dei parametri di funzionamento durante i controlli dei dispositivi medici in ospedale, nonché per la trasmissione dal domicilio del paziente dei dati rilevati al monitoraggio remoto, anche se in quest’ultimo caso un’eventuale breccia nel sistema potrebbe compromettere i dati sensibili dei pazienti e non la programmazione o il funzionamento dei dispositivi.

Non essendo dotato di sistemi di sicurezza sofisticati nei confronti di possibili cyber attacchi, il sistema renderebbe teoricamente possibile ad un tentativo di hackeraggio di accedere alle informazioni sensibili del paziente ed alla programmazione o estrapolazione di dati.

Al momento attuale non è stato osservato nessun episodio di cyberattacco, né di violazione della privacy, e tantomeno nessun evento che abbia portato un rischio reale alla salute di alcun paziente. In relazione all’avviso di sicurezza la Food and Drug administration non ha ritenuto di intervenire sull’uso dei device, fornendo indicazioni generali di prudenza per l’uso del sistema.

Dal punto di vista pratico le teoriche vulnerabilità del sistema non sembrano comportare problemi o pericoli reali nella gestione dei pazienti.
La trasmissione per RF è possibile solo in presenza di una limitata distanza tra device e programmatore/trasmettitore e le possibili interferenze o intromissioni richiederebbero la presenza

dell'eventuale esecutore dell'attacco in diretta vicinanza del portatore del dispositivo. Tale evenienza sembra da escludersi in ambiente sanitario e/o ospedaliero, sede in cui avvengono tali operazioni.

In caso di monitoraggio remoto, la trasmissione di dati tra device e trasmettitore avviene a domicilio del paziente e potrebbe risultare più suscettibile di intromissioni non autorizzate nel sistema. In questo caso comunque l'attivazione avviene in finestre temporali limitate, variabili da paziente a paziente e totalmente non predicibili per soggetti esterni.
In definitiva, pur in presenza di una potenziale vulnerabilità del sistema, il rischio risulta essere realisticamente estremamente limitato.

Suggerimenti AIAC

L'AIAC suggerisce agli operatori un comportamento nella gestione del problema improntato alla prudenza, valutando il potenziale impatto del problema tecnico nel singolo paziente.
Al momento attuale non esiste indicazione ad una variazione della pratica clinica. Non è indicata alcuna azione correttiva a carico dei device impiantati.
Si suggerisce comunque:

- Utilizzare esclusivamente materiale di provenienza dell'azienda interessata.
- Assicurarsi che i programmatori ed il materiale di trasmissione siano situati nella struttura sanitaria in un luogo sicuro e non accessibile per altri che non il personale sanitario.
- Verificare che i computer utilizzati per la gestione del monitoraggio remoto ed i server della struttura sanitaria siano adeguatamente protetti con software contro virus o accessi non autorizzati.
- Tenere traccia dei dati rilevati a controlli e monitoraggio remoto per verificare possibili anomalie.
- Dare immediata segnalazione di possibili eventi correlati alle autorità competenti come incidenti o mancati incidenti

02 maggio 2019

Ezio Soldati
Chairman della Task Force
"Avarie e Complicanze"

Renato Pietro Ricci
Presidente AIAC
a nome del Consiglio Direttivo