Notifica di Sicurezza sul Campo

FSN-CMS8000

Nome della marca	Contec	**Modello e Nome del Prodotto**	CMS8000 Monitor del Paziente
SN/LOT	Vedere l'allegato	**Data**	10/02/2025

Descrizione del Problema:

Recentemente, la nostra azienda ha appreso da FDA e CISA che il monitor del paziente CMS8000 presenta le seguenti vulnerabilità di sicurezza:

1. Il monitor del paziente potrebbe essere controllato remotamente da un utente non autorizzato o non funzionare come previsto.

2.Il software sui monitor dei pazienti include una backdoor, il che significa che il dispositivo o la rete a cui il dispositivo è stato connesso potrebbe essere stato compromesso o potrebbe essere compromesso in futuro.

3.Una volta che il monitor del paziente è connesso a Internet, inizia a raccogliere i dati dei pazienti, inclusi dati di identificazione personale (PII) e informazioni sulla salute protette (PHI), e a trasferirli (withdrawing) al di fuori dell'ambiente di erogazione sanitaria.

Al momento, Contec non è a conoscenza di alcun incidente di sicurezza, infortunio o morte correlato a queste vulnerabilità di sicurezza.

Tuttavia, considerando che queste vulnerabilità di sicurezza possono mettere i pazienti a rischio quando il monitor paziente è connesso a Internet, in conformità con le regolamentazioni EU MDR e i procedure di controllo aziendali pertinenti, emettiamo questa Notifica di Sicurezza sul Campo (FSN).

Impatto:

Il CMS8000 monitor paziente è destinato a essere utilizzato per il monitoraggio, la visualizzazione, la revisione, l'archiviazione e l'allarme di diversi parametri fisiologici, tra cui ECG, frequenza cardiaca, frequenza respiratoria, pressione sanguigna non invasiva, pressione sanguigna invasiva, anidride carbonica e temperatura di adulti, pazienti pediatrici e neonati. Se la vulnerabilità viene sfruttata, potrebbe portare ai seguenti problemi:

- L'interruzione della monitorizzazione continua dei segni vitali ha causato un ritardo nella scoperta delle condizioni critiche del paziente, con conseguente ritardo dell'intervento medico.
- Manipolazione o corruzione dei dati trasmessi dal monitor paziente, portando a letture errate e potenzialmente a decisioni mediche dannose basate su dati falsi.

Chiunque abbia ricevuto questa notifica e risulti essere interessato da questa vulnerabilità, è pregato di intraprendere le seguenti misure di mitigazione:

1. Se il dispositivo dell'utente è attualmente in uso autonomo e non ci sono piani di connetterlo a una rete (compresa una rete cablata o wireless), l'utente può temporaneamente rimandare questo aggiornamento. Tuttavia, una volta che ci saranno piani di connettere il dispositivo a una rete in futuro, è pregato di scaricare immediatamente il pacchetto di aggiornamento software inviato dalla nostra azienda e installarlo secondo la guida di aggiornamento software per garantire la sicurezza del sistema.

2.Se il dispositivo dell'utente si trova in una rete locale chiusa (LAN) che è fisicamente isolata da Internet e non sono collegate altre apparecchiature oltre i dispositivi medici, il rischio di sicurezza di

rete in questo ambiente è estremamente basso. In questo caso, l'utente può decidere se scaricare e installare il pacchetto di aggiornamento software in base alla situazione effettiva. Se ci saranno piani di connettere il dispositivo a una rete privata non chiusa in futuro, è pregato di scaricare immediatamente il pacchetto di aggiornamento software inviato dalla nostra azienda e installarlo secondo la guida di aggiornamento software per garantire la sicurezza del sistema.
3.Se il dispositivo dell'utente non è utilizzato in un ambiente di rete sicuro (cioè non in una rete locale chiusa (LAN) che è fisicamente isolata da Internet e connessa solo ad altri dispositivi medici), è pregato di intraprendere Azioni immediate o intraprendere Azioni di mitigazione a lungo termine:
a. Azioni immediate: Si consiglia di adottare la misura di disconnettersi in modo sicuro dalla rete staccando il cavo di rete e di abilitare solo la funzione di monitoraggio locale.
b. Azioni di mitigazione a lungo termine: È pregato di scaricare immediatamente il pacchetto di aggiornamento software inviato dalla nostra azienda e installarlo secondo la guida di aggiornamento software per garantire la sicurezza del informatica.

Come identificare i prodotti interessati:

Si prega di controllare il numero di serie del dispositivo utilizzato e l'allegato “Informazioni sul Prodotto Interessato”. Se il dispositivo utilizzato è elencato nell'allegato, si tratta di un dispositivo interessato.

Informazioni di Contatto:

Se avete alcune domande, potete contattarci in qualsiasi momento via e-mail. E-mail: contec_monitor@contecmed.com. Vi risponderemo prontamente e lavoreremo con voi per risolvere il problema.

Nota：
Questa Notifica di Sicurezza sul Campo deve essere condivisa con chiunque debba essere informato all'interno della vostra organizzazione e inoltrata a qualsiasi organizzazione dove i dispositivi potenzialmente interessati sono stati trasferiti.

Redatto da: Xiao Jie

Approvato da:Yang Zhishan (Direttore Generale) firma:

Contec Medical Systems Co., Ltd.

Data:10-02-2025