REGIONE DEL VENETO

giunta regionale

Data 27/02/2025 Protocollo N° 0102141 Class: G.930.01 Fasc. Allegati N° 4

Oggetto: Circolare del Ministero della Salute prot. n. 0010860 del 07/02/2025 - Rilevata backdoor nel dispositivo medico MONITOR PAZIENTE - CMS8000. **Aggiornamento**

Ai Direttori Generali Aziende ULSS, Aziende Ospedaliere, IRCSS della Regione del Veneto
All'A.R.I.S.
All'A.I.O.P.
All'A.N.I.S.A.P.
Agli Ordini dei Medici Chirurghi
Alle Organizzazioni sindacali dei Medici di Assistenza Primaria
Alle Organizzazioni sindacali dei medici Pediatri di Libera Scelta
Federazione Ordine Farmacisti Italiani

e p.c. Al Direttore Generale Area Sanità e Sociale
Al Direttore Direzione Programmazione Sanitaria – LEA
Al Direttore Generale Azienda Zero

Con la presente, si fa seguito alla nota prot. 0078592 del 13/02/2025, con la quale la scrivente Direzione aveva trasmesso la Circolare ministeriale, di cui all'oggetto, concernente una comunicazione urgente del Ministero della Salute relativa al dispositivo medico **MONITOR PAZIENTE CMS8000 - CONTEC MEDICAL SYSTEMS CO. LTD.**

Come già anticipato con comunicazione via email in data 21/02/2025, il Ministero della Salute ha comunicato che, a seguito di ulteriori approfondimenti, l'avviso di sicurezza n. FSN-CMS8000 coinvolge, oltre ai dispositivi con codice CMS8000 menzionati nella precedente nota, anche i monitor con codice CMS6500 e CMS7000. Il fabbricante ha reso disponibile l'avviso aggiornato (FSN-EU202501) in lingua italiana, che si allega alla presente, unitamente alla documentazione completa, reperibile anche sul sito web del Ministero.

Si richiede pertanto alle SS.LL. di prendere attenta visione della documentazione allegata, al fine di provvedere tempestivamente ad informare tutti gli utenti che utilizzano i dispositivi in questione, assicurando la messa in atto delle azioni previste.

Ringraziando per la collaborazione, si porgono cordiali saluti.

Il Direttore
Direzione Farmaceutico-Protesica-Dispositivi Medici
Dott.ssa Giovanna Scroccaro

Referente della materia: dott.ssa Rita Mottola tel 041 2793515
Referente della pratica: dott.ssa Francesca Bassotto tel 041.2791450

Area Sanità e Sociale
Direzione Farmaceutico – Protesica – Dispositivi Medici
Rio Novo, Dorsoduro 3493 – 30123 Venezia Tel. 041.2793412-3415-3406-1453 – Fax n. 041.2793468
PEC: *area.sanitasociale@pec.regione.veneto.it e-mail: assistenza.farmaceutica@regione.veneto.it*
Cod. Fisc. 80007580279 ***fatturazione elettronica - Codice Univoco Ufficio*** *GIIHNV P.IVA 02392630279*

Notifica di Sicurezza sul Campo

FSN-EU202501

Nome della marca	Contec	**Data**	24/02/2025
Nome del Prodotto	Monitor del Paziente	**Modello**	CMS6000/CMS6500/CMS7000/ CMS8000/CMS9000

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 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

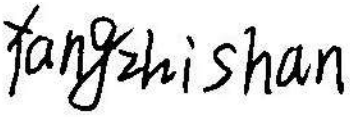
installare il pacchetto di aggiornamento software in base alla situazione effettiva. Se ci saranno piani di connettere il dispositivo a una rete privata non chiusa in futuro, è pregato di scaricare immediatamente il pacchetto di aggiornamento software inviato dalla nostra azienda e installarlo secondo 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: Una volta che avete confermato che il vostro monitor necessita di un aggiornamento, non esitate a contattare il distributore locale o la nostra azienda via e-mail. E-mail della nostra azienda: contact@contecmed.com. Vi forniremo prontamente il pacchetto di aggiornamento e la guida per l'installazione. Per garantire un processo fluido, vi preghiamo di avere a disposizione i dettagli del prodotto, come il modello, l'UDI o il numero di serie (SN), che possono essere generalmente trovati sul retro del dispositivo o nella confezione. Se avete domande o necessitate ulteriore assistenza, non esitate a contattarci in qualsiasi momento. Siamo qui per aiutarvi.

Informazioni di Contatto:

Se avete alcune domande, non esitate a contattare la nostra azienda via e-mail.E-mail: contact@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:24-02-2025

Ministero della Salute

DIPARTIMENTO DELLA PROGRAMMAZIONE DEI DISPOSITIVI MEDICI DEL SERVIZIO DEL FARMACO E DELLE POLITICHE IN FAVORE DEL SERVIZIO SANITARIO NAZIONALE

EX DIREZIONE GENERALE DEI DISPOSITIVI MEDICI E DEL SERVIZIO FARMACEUTICO

Lista di distribuzione

Assessorati alla Sanità delle Regioni e Province autonome **PEC** **Istituto Superiore di Sanità – ISS** **PROTOCOLLO.CENTRALE@PEC.ISS.IT** **Comando Carabinieri per la Sanità** **srm20400@pec.carabinieri.it** **FNOMCeO** Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri **segreteria@pec.fnomceo.it** **FOFI** Federazione Ordine Farmacisti Italiani **posta@pec.fofi.it** **FNOPI** Federazione Nazionale Ordini Professioni Infermieristiche **federazione@cert.fnopi.it** **FNOPO** **presidenza@pec.fnopo.it** **FEDERFARMA** Federazione nazionale unitaria titolari di farmacia **federfarma@pec.federfarma.it** **F.I.M.M.G.** Federazione Italiana Medici di Medicina Generale **segreteria@fimmg.org**	**F.I.S.M.** Federazione Italiana delle Società Medico scientifiche **Fism.pec@legalmail.it** **SIFO** Società Italiana Farmacia Ospedaliera **sifosede@sifoweb.it** **AIFA** **direzione.generale@pec.aifa.gov.it** **AGENAS** **agenas@pec.agenas.it** **A.I.P.O. - ITS** Associazione Italiana Pneumologi Ospedalieri *Italian Thoracic Society* **direzionegenerale@aiporicerche.it** **aiposegreteria@aiporicerche.it** **S.I.A.A.R.T.I.** Società Italiana di Anestesia, Analgesia, Rianimazione e Terapia Intensiva **segreteria@siaarti.it** **Ministero della Difesa** **Dir. Gen. Sanità Militare** **stamadifesa@postacert.difesa.it** **Confindustria Dispositivi Medici** **confindustriadm@pec.confindustriadm.it**

FNO TSRM e PSTRP Federazione nazionale degli ordini dei tecnici sanitari di radiologia medica e delle professioni sanitarie tecniche, della riabilitazione e della prevenzione **federazione@pec.tsrm.org** **F.I.A.S.O.** La Federazione Italiana Aziende Sanitarie e Ospedaliere **webmaster@fiaso.it** **A. I. O. P.** Associazione Italiana Ospedalità Privata **Segreteria.generale@aiop.it** **A.N.M.D** Associazione Nazionale Medici Direzioni Ospedaliere **anmdo.segreteria@gmail.com** **A. I. M. E. F.** Associazione Italiana dei Medici di Famiglia **mail@aimef.org** **ACOI** Associazione Chirurghi Ospedalieri Italiani **segreteria@acoi.it** **acoi@legalmail.it** **SITI** Società Italiana Terapia Intensiva **gconsales@gmail.com** **A.N.M.I.R.S.** Associazione Nazionale Medici Istituti Religiosi Spedalieri **info@anmirs.it**	**E p.c.** **Ufficio di Gabinetto** **Ufficio Stampa**

OGGETTO: RILEVATA BACKDOOR NEL DISPOSITIVO MEDICO MONITOR PAZIENTE CMS8000

MOTIVO DELLA COMUNICAZIONE:

La scrivente Direzione generale è stata informata che il dispositivo medico MONITOR PAZIENTE CMS8000 contiene una backdoor che potrebbe trasmettere i dati dei pazienti a un indirizzo IP remoto. Questa vulnerabilità rappresenta un grave rischio per la sicurezza, poiché un monitor compromesso potrebbe pregiudicare la corretta risposta ai segni vitali del paziente e questi ultimi essere manipolati da remoto.

La *Cybersecurity and Infrastructure Security Agency* (CISA) che ha rilevato la problematica, ne ha dato comunicazione al seguente link: **https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf**

Ad oggi, nessun incidente di cybersecurity o di manomissione del dispositivo in oggetto è stato segnalato alla ex Direzione generale dei dispositivi medici e del servizio farmaceutico

INDICAZIONI:

Si invitano i Medici di medicina generale (MMG), i Pediatri di libera scelta (PLS) e tutte le strutture sanitarie pubbliche e private operanti sul territorio a mettere in atto ogni azione volta a:

- verificare la presenza del dispositivo in oggetto presso i loro assistiti;
- se possibile, scollegare il dispositivo dalla rete;
- controllare il dispositivo al fine di rilevare eventuali segni di manomissione come, ad esempio, la visualizzazione di informazioni sul monitor non coerenti con le condizioni cliniche dell'assistito.

Si invitano i *caregiver* e tutti gli utilizzatori di monitor multiparametrici a domicilio a verificare se il dispositivo in uso sia un MONITOR PAZIENTE CMS8000. In tal caso, è necessario comunicare tale rilievo al proprio MMG o PLS per gli accertamenti di competenza.

Un'eventuale manomissione individuata sul MONITOR PAZIENTE CMS8000 rappresenta un incidente grave e pertanto soggiace all'obbligo di segnalazione al Ministero della salute ai sensi dell'art.10 del Dlgs 137/2022, secondo termini e modalità di cui alla circolare 29 novembre 2022 (per info: https://www.salute.gov.it/portale/dispositiviMedici/dettaglioContenutiDispositiviMedici.jsp?lingua=italiano&id=26&area=dispositivi-medici&menu=vigilanza).

Si invitano tutti gli altri enti in indirizzo a dare massima diffusione al documento stesso.

Il DIRETTORE GENERALE

Dott. Achille IACHINO

2025.02.07 18:03:12
Dott. Achille Iachino
Ministero della Salute

Rif: Dott.ssa Antonella Campanale

Direttore incaricato Ufficio 5 - DGDMF

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

REGIONE DEL VENETO

giunta regionale

Data 13/02/2025 Protocollo N° 0078592 Class: G.930.01 Fasc. Allegati N° 1

Oggetto: Circolare del Ministero della Salute prot. n. 0010860 del 07/02/2025 - Rilevata backdoor nel dispositivo medico MONITOR PAZIENTE - CMS8000. **Trasmissione**

Ai Direttori Generali Aziende ULSS, Aziende Ospedaliere, IRCSS
All'A.R.I.S.
All'A.I.O.P.
All'A.N.I.S.A.P.
Agli Ordini dei Medici Chirurghi
Alle Organizzazioni sindacali dei Medici di Assistenza Primaria
Alle Organizzazioni sindacali dei medici Pediatri di Libera Scelta
Federazione Ordine Farmacisti Italiani

e p.c. Al Direttore Generale Area Sanità e Sociale
Al Direttore Direzione Programmazione Sanitaria – LEA
Al Direttore Generale Azienda Zero

Con la presente si trasmette in allegato la Circolare ministeriale, di cui all'oggetto, concernente una comunicazione urgente del Ministero della Salute relativa al dispositivo medico **MONITOR PAZIENTE CMS8000 - CONTEC MEDICAL SYSTEMS CO. LTD.**

In particolare, il Ministero segnala una potenziale problematica riguardante tale dispositivo, ovvero la possibile trasmissione dei dati dei pazienti a un indirizzo IP remoto senza autorizzazione, con conseguente malfunzionamento del monitor.

Si chiede pertanto alle SS.LL. di prendere attenta visione della suddetta Circolare Ministeriale, dandone massima diffusione a tutti gli interessati, nonché di assicurare la messa in atto di tutte le azioni in essa previste.

La scrivente si impegna a fornire tempestivamente eventuali aggiornamenti relativi alla presente comunicazione.

L'occasione è gradita per porgere cordiali saluti.

Il Direttore
Direzione Farmaceutico-Protesica-Dispositivi Medici
Dott.ssa Giovanna Scroccaro

Referente della materia: dott.ssa Rita Mottola tel 041 2793515
Referente della pratica: dott.ssa Francesca Bassotto tel 041.2791450

Area Sanità e Sociale
Direzione Farmaceutico – Protesica – Dispositivi Medici
Rio Novo, Dorsoduro 3493 – 30123 Venezia Tel. 041.2793412-3415-3406-1453 – Fax n. 041.2793468
PEC: *area.sanitasociale@pec.regione.veneto.it e-mail: assistenza.farmaceutica@regione.veneto.it*
Cod. Fisc. 80007580279 ***fatturazione elettronica - Codice Univoco Ufficio*** *GIIHNV P.IVA 02392630279*