Notatka Bezpieczeństwa

FSN-EU202501

Nazwa marki	Contec	**Data**	2025/02/24
Nazwa produktu	Monitor Pacjenta	**Model**	CMS6000/CMS6500/CMS7000/ CMS8000/CMS9000

Opis problemu:

Niedawno nasza firma dowiedziała się od FDA I CISA, że monitor pacjenta CMS8000 ma następujące luki w zabezpieczeniach cyberbezpieczeństwa:

1. Monitor pacjenta może być zdalnie sterowany przez nieautoryzowanego użytkownika lub nie działać jak powinien.
2. Oprogramowanie monitorów pacjenta zawiera backdoora, co może oznaczać, że urządzenie lub sieć do której podłączone jest urządzenie mogły zostać naruszone.
3. Po podłączeniu monitora pacjenta do Internetu, skompromitowane urządzenie zaczyna zbierać informacje o danych pacjenta, w tym wrażliwych danych osobowych (PII) I chronionych informacji o stanie zdrowia (PHI) a następnie rozpoczyna ich exflitracje (przesyłanie) poza środowisko świadczenia opieki zdrowotnej.

Do tej pory Contec nie ma informacji o żadnych incydentach bezpieczeństwa, obrażeniach ani zgonach powiązanych z tymi podatnościami.

Biorąc jednak pod uwagę, że te podatności mogą narazić pacjentów na ryzyko gdy monitor pacjenta jest podłączony do Internetu, zgodnie z przepisami EU MDR I odpowiednimi procedurami kontrolnymi firmy, publikujemy niniejszą Informację o bezpieczeństwie (FSN).

Wpływ:

Monitor pacjenta jest przeznaczony do monitorowania, wyświetlania, oceniania, przechowywania i alarmowania wielu parametrów fizjologicznych, w tym EKG, częstości akcji serca, częstości oddechów, nieinwazyjnego ciśnienia krwi, inwazyjnego ciśnienia krwi, dwutlenku węgla i temperatury u pacjentów dorosłych, dzieci i noworodków. Jeśli podatność zostanie wykorzystana, może to doprowadzić do następujących zdarzeń:

- Zakłócenie ciągłego monitorowania parametrów życiowych, prowadzące do opóźnienia w wykrywaniu krytycznych zmian w stanie zdrowia pacjenta i opóźnionej interwencji medycznej.
- Manipulacja lub uszkodzenie danych przesyłanych przez monitor pacjenta, prowadzące do nieprawidłowych odczytów i potencjalnie szkodliwych decyzji medycznych opartych na fałszywych danych.

Osoby które otrzymały to powiadomienie I zostały uznane za dotknięte tą podatnością powinny podjąć następujące działania zaradcze:

1. Jeśli urządzenie użytkownika jest obecnie używane samodzielnie i nie ma planów podłączenia go do żadnej sieci (w tym sieci przewodowych lub bezprzewodowych), użytkownik może tymczasowo odłożyć to na później. Jednak gdy pojawią się plany podłączenia urządzenia do sieci w przyszłości, prosimy o niezwłoczne pobranie pakietu aktualizacji oprogramowania wysłanego przez naszą firmę i zainstalowanie go zgodnie z przewodnikiem aktualizacji oprogramowania, aby zapewnić cyberbezpieczeństwo.
2. Jeśli urządzenie użytkownika znajduje się w zamkniętej sieci lokalnej (LAN) która jest fizycznie odizolowana od Internetu i żadne inne urządzenia poza urządzeniami medycznymi nie są podłączone do tej sieci, ryzyko zagrożenia sieci w takim środowisku jest wyjątkowo niskie. W takim

przypadku użytkownik może zdecydować, czy pobrać i zainstalować pakiet aktualizacji oprogramowania zgodnie z rzeczywistą sytuacją. Jeśli istnieją plany podłączenia urządzenia do niezamkniętej sieci prywatnej w przyszłości, prosimy o niezwłoczne pobranie pakietu aktualizacji oprogramowania wysłanego przez naszą firmę i zainstalowanie go zgodnie z przewodnikiem aktualizacji oprogramowania, aby zapewnić cyberbezpieczeństwo.

3. Jeżeli urządzenie użytkownika nie jest używane w bezpiecznym środowisku sieciowym (tj. nie w zamkniętej sieci lokalnej (LAN), która nie jest fizycznie odizolowana od Internetu i do której nie są podłączone żadne inne urządzenia poza urządzeniami medycznymi), należy podjąć następujące natychmiastowe i długoterminowe działania:

a. Natychmiastowe działania: Zaleca się podjęcie kroków w celu bezpiecznego odłączenia się od sieci poprzez odłączenie kabla sieciowego i włączenie samej funkcji monitorowania lokalnego.

b. Długoterminowe działania łagodzące: Po potwierdzeniu, że aktualizacja monitora jest konieczna, nie wahaj się skontaktować z lokalnym dystrybutorem lub naszą firmą za pośrednictwem poczty e-mail. Adres e-mail naszej firmy: contact@contecmed.com. Niezwłocznie przekażemy Ci pakiet aktualizacji i instrukcję instalacji. Aby zapewnić płynny proces, przygotuj dane dotyczące produktu, takie jak model, UDI lub SN, które zazwyczaj można znaleźć z tyłu urządzenia lub na opakowaniu. Jeśli masz jakiekolwiek pytania lub potrzebujesz dalszej pomocy, skontaktuj się z nami w dowolnym momencie. Jesteśmy tutaj, aby pomóc.

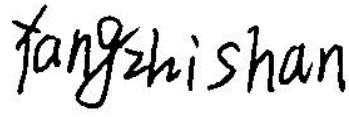
Informacje Kontaktowe:

Jeśli masz jakiekolwiek pytania, nie wahaj się skontaktować z naszą firmą przez e-mail. E-mail: contact@contecmed.com. Skontaktujemy się z Tobą niezwłocznie i wspólnie rozwiążemy problem.

Uwaga：

Niniejszą Informację o bezpieczeństwie należy udostępnić wszystkim osobom w organizacji, które powinny o niej wiedzieć oraz przesłać ją do każdej organizacji do której przeniesiono potencjalnie zainfekowane urządzenia.

Opracował: Xiao Jie 

Zatwierdzone przez: Yang Zhishan (Menedżer Generalny) Podpis: 

Contec Medical Systems Co., Ltd.
Data:2025-2-24