ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Backdoor dans les solutions de surveillance médicales « Contec CMS8000 » et « Epsimed MN-120 »
Numéro de Référence	52320302/25
Date de publication	03 Février 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- CMS8000 Patient Monitor: Firmware version smart3250-2.6.27-wlan2.1.7.cramfs
- CMS8000 Patient Monitor: Firmware version CMS7.820.075.08/0.74(0.75)
- CMS8000 Patient Monitor: Firmware version CMS7.820.120.01/0.93(0.95)
- CMS8000 Patient Monitor: Toutes les versions (CVE-2025-0626, CVE-2025-0683)
- Epsimed MN-120

Identificateurs externes

- CVE-2025-0626 CVE-2024-12248 CVE-2025-0683

Bilan de la vulnérabilité

L'Agence de cybersécurité et de sécurité des infrastructures « CISA » et le Département de la Santé et des Services Humains des États-Unis « FDA », annoncent la découverte d'un « Backdoor » affectant les solutions de surveillance médicales « Contec CMS8000 » et « Epsimed MN-120 ».

Ces deux solutions permettent la surveillance des signes vitaux des patients comme la respiration, le pouls, la pression artérielle, la température corporelle et la saturation du sang en

oxygène.

La vulnérabilité en relation avec le Backdoor identifiée par « CVE-2025-0626 » ouvre un accès à distance vers une adresse IP codée en dur sur l'équipement vulnérable s'il est connecté à Internet. Cela permet à un acteur malveillant de télécharger et d'écraser des fichiers sur l'appareil.

En plus du « Backdoor », deux autres vulnérabilités critiques ont été identifiées sur les équipements susmentionnés. L'exploitation de ces vulnérabilités peut permettre à attaquant distant d'exécuter du code arbitraire ou d'exfiltrer des donnés sensibles.

Solution

Aucune mise à jour de sécurité n'est disponible pour le moment. Cependant, il est recommandé de :

- Déconnecter les équipements « Contec CMS8000 » et « Epsimed MN-120 » d'Internet immédiatement
- Minimisez l'exposition du réseau pour tous les appareils et/ou systèmes du système de contrôle, en vous assurant qu'ils ne sont pas accessibles depuis Internet
- Localiser les réseaux du système de contrôle et les appareils distants derrière des pare-feu et les isoler des réseaux d'entreprise
- Mettez à jour les règles de pare-feu pour empêcher l'accès aux appareils potentiellement concernés

Risques

- Exfiltration et modification de données sensibles
- Exécution de code arbitraire à distance

Références

Bulletins de sécurité de « CISA » et de « FDA »:

- https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication#reporting
- https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-030-01