

**EOVE SA**  
Bâtiment NEWTON  
4 rue Jules FERRY  
64000 PAU - France

A l'attention du Correspondant de Matéiovigilance

**Pau, 3 septembre 2018**

**Objet : Information importante de sécurité concernant le ventilateur EO-150 utilisé avec les technologies de communication sans fil.**

**Référence dossier : R1813968**

Chers clients,

Par ce courrier, nous vous adressons une information importante de sécurité concernant la connexion Bluetooth du ventilateur **EO-150**, notamment lorsqu'elle est utilisée pour l'application smartphone EO-VisioControl.

Afin d'apporter la meilleure sécurité à tous les patients ventilés avec l'EO-150, nous vous demandons de diffuser cette information à tous les membres de vos équipes impliqués dans l'utilisation du ventilateur EO-150.

Comme vous avez pu en prendre conscience par vous-même, les cas de cyberattaques rapportés dans les médias augmentent, menaçant les technologies informatiques connectées, et notamment les dispositifs médicaux utilisant les transmissions radios comme le Bluetooth ou le WIFI.

Le Bureau fédéral de Sécurité de l'Information en Allemagne (BSI), est à l'initiative d'une investigation lancée depuis plusieurs mois mettant en œuvre un scénario de cyberattaque vis à vis de notre dispositif EO-150 comme pour d'autres dispositifs médicaux.

Suite à la réception de son rapport concernant l'EO-150, nous avons pu analyser en profondeur ses conclusions, notamment pour les connexions Bluetooth utilisées par le ventilateur.

Aussi, nous avons pu identifier une vulnérabilité potentielle due à la connexion Bluetooth utilisée pour l'application smartphone EO-VisioControl du ventilateur EO-150. Il est important de préciser, qu'à ce jour aucun incident n'a été rapporté invoquant cette potentielle vulnérabilité.

Néanmoins, dans ce cadre, EOVE a décidé de déployer une Action Corrective de Sécurité sur le Terrain pour tous les ventilateurs EO-150 mis en service. Nous mettons d'ores et déjà tout en œuvre pour fournir dans les meilleurs délais cette action corrective.

Nous vous prions par avance de nous excuser pour la gêne occasionnée par cette action de sécurité. Votre contact habituel reste à votre écoute pour répondre à vos questions et demandes individuelles.

Vous pouvez également contacter directement notre standard EOVE au (+33).5.59.21.86.84

Nous vous prions d'agréer, Madame, Monsieur, l'expression de nos sincères salutations

**Fabien Cotteaux,**  
Directeur Général

**Patrick Dehour,**  
Directeur Qualité



**Information importante de sécurité concernant le ventilateur EO-150 utilisé avec les technologies de communication sans fil.**

**R1813968**

---

**Description du problème** Vulnérabilité potentielle à une cyberattaque des connexions sécurisées sans fil Bluetooth du ventilateur EO-150, dans le cadre de l'utilisation de l'application smartphone EO-VisioControl.  
L'utilisation du module de ventilation EO-150 connecté à la Docking Station ou EO-Remote VISION TABLET supprime cette vulnérabilité.

---

**Produits concernés** Ventilateurs **EO-150 (réf. EO-150VNT)**  
Application Smartphone **EO-VisioControl (réf. EO-VISIOSMA)**

---

**Information sur le risque potentiel** Aucun incident terrain en relation avec cette potentielle vulnérabilité n'a été rapporté à ce jour.  
Par conséquent, EOVE considère le risque potentiel associé comme acceptable avec la mise en place des actions préventives immédiates.  
De fait, nous proposons les actions décrites ci-dessous.

---

**Actions Préventives immédiates** **Pour tous les patients, suspension** de l'utilisation de l'application Smartphone **EO-VisioControl** avec le ventilateur EO-150 jusqu'à mise à disposition de la nouvelle application. A ce titre, l'application n'est plus disponible en téléchargement à partir de notre site.

**Pour les patients ventilo-dépendants**, nous vous demandons d'utiliser le module de ventilation EO-150 connecté en continu avec la DOCKING STATION EO-150 ou la tablette EO-REMOTE VISION.

Et ce jusqu'à mise en œuvre de l'action corrective décrite au paragraphe suivant.

**Actions  
Correctives**

L'Action Corrective obligatoire inclut les évolutions logicielles suivantes :

- Retrait de l'application smartphone EO-VisioControl actuelle.
- Implémentation d'un nouveau protocole de connexion Bluetooth plus performant, avec clés de sécurité aléatoires générées à la première connexion entre le module de ventilation EO-150 et sa DOCKING STATION EO-150 ou sa tablette EO-REMOTE VISION.
- Cryptage des données configurées pour le WiFi utilisé dans le logiciel embarqué de la DOCKING STATION EO-150 et de la tablette EO-REMOTE VISION.
- L'implémentation d'une nouvelle connectivité Bluetooth plus performante du module de ventilation EO-150, pour se connecter à la DOCKING STATION EO-150 propriétaire et à la tablette EO-REMOTE VISION propriétaire.

---

**Délai de  
mise en  
oeuvre**

Le pack logiciel apportant les améliorations de connectivité sera disponible à partir du 1er novembre 2018.

Dès le 1er novembre 2018, tous les dispositifs sortant de notre site de production et mis sur le marché bénéficieront de cette évolution logicielle.

Concernant la mise à jour de la base installée, nous demandons à nos clients de mettre à jour les dispositifs concernés lors de la prochaine maintenance (sous 12 mois), à partir de sa date de mise à disposition.

Une nouvelle application smartphone sera mise à votre disposition ultérieurement.

---

## FORMULAIRE DE RÉPONSE CLIENT

Notice de Sécurité Importante en date du 3 septembre 2018 - R1813968

### Ventilateur EO-150

**Désignation des produits :** EO-150 Ventilator

**Code produits :**EO-150VNT

Veillez compléter et renvoyer sans délai le présent formulaire

par fax : 05 59 84 42 96

ou par email : [contact@eove.fr](mailto:contact@eove.fr)

Nom et adresse de l'établissement :	
Nom du contact :	
Titre :	
Email et numéro de téléphone :	

**Nous accusons réception de cette notice de sécurité R1813968 et nous confirmons :**

- 1. avoir compris son contenu**
- 2. avoir diffusé cette information aux personnes concernées.**

<b>Nom de la personne :</b>	<b>Signature :</b>	<b>Date :</b>