AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Information évènement – Vigilance e-CPS

A destination : Autorités d'enregistrement – usage interne

Le 08/10/2025,

L'EVENEMENT

Plusieurs utilisations frauduleuses de l'application mobile e-CPS et du portail ProSantéConnect (PSC) ont été identifiées, incluant des situations d'usurpation de l'application mobile e-CPS auprès de leur porteur légitime par un procédé d'ingénierie sociale.

La méthode observée consiste en un contact direct d'un professionnel de santé par un fraudeur en se faisant passer pour « le service client CPS », permettant l'obtention des informations pour la génération d'une e-CPS via l'application mobile (QR Code communiqué par mail et un code communiqué par SMS, issus des données déclarées dans le RPPS). Le fraudeur a ainsi pu abuser de la confiance du professionnel de santé en détournant ses moyens d'authentification.

Dans la continuité de l'attaque sur les ENRS (Espaces Numériques Régionaux de Santé) des GRADeS, nous assistons à de nouvelles tentatives d'usurpation d'identité de professionnels de santé. Le/les fraudeur(s) est motivé et a pu mettre en œuvre des méthodes éprouvées, comme dans les secteurs bancaires ou télécom, qui portent malheureusement leurs fruits dans notre domaine de la santé. Le nombre de cas identifiés reste, à ce jour, très limité, moins d'une quinzaine de cas à ce stade pour plus de 500 000 e-CPS, mais les attaquants restent actifs.

- Les investigations techniques menées par l'ANS, en lien avec l'Assurance Maladie et les GRADeS (Groupements Régionaux d'Appui au Développement de la eSanté), confirment qu'aucune faille technique n'a été constatée dans les systèmes ProSantéConnect, ni dans le processus d'enrôlement ou d'utilisation de la e-CPS.

- **L'ANS a immédiatement pris les mesures nécessaires :**
  - Désactivation des e-CPS concernées,
  - Blocage des nouvelles générations associées,
  - Contact individuel des professionnels impactés,
  - Mobilisation du service client et des experts cybersécurité pour assurer suivi et accompagnement.

LE DISPOSITIF MIS EN PLACE

À ce jour, et malgré l'impact limité, nous avons mobilisé et mis en place une Task Force interne pour faire face à cette situation. Ce type de cas, pour l'heure à l'impact mineur et limité, est pris très au sérieux par l'ANS. Il s'agit, notamment à travers notre mission de régulateur, d'assurer la sécurité des systèmes d'information et de tous les moyens qui permettent d'accéder aux données des professionnels de santé et des patients.

Nous restons pleinement engagés dans notre rôle de fournisseur d'identité, en appui des fournisseurs de services, et poursuivons nos efforts de sensibilisation pour garantir la sécurité des accès numériques en santé.

Dans ce cadre, des actions **de sensibilisation ciblées** sont en cours et seront renforcées dans les prochaines semaines.

Les bons usages à rappeler aux professionnels de santé

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 08 06 80 02 13
esante.gouv.fr

Afin de réduire au maximum les risques de fraude, nous vous remercions de relayer les consignes suivantes :

- Ne jamais communiquer ses identifiants e-CPS par téléphone.
- Ne jamais transmettre de codes reçus par SMS ou email.
- Ne jamais partager l'écran de son ordinateur ou de son smartphone.
- Vérifier régulièrement que ses coordonnées (email, téléphone) sont à jour auprès de son Ordre ou autorité d'enregistrement.

Il est important de rappeler que **ni l'ANS, ni les ARS, ni aucun autre acteur institutionnel** ne demandera jamais ce type d'informations sensibles par téléphone ou par mail.

Des messages de bonnes pratiques sont affichés depuis le 17 septembre sur la page d'accueil d'esante.gouv.fr ainsi que sur la mire de connexion ProSanteConnect. De même, des posts de sensibilisation ont été diffusés via les réseaux sociaux. Concomitamment, et sur le même principe que la communication de l'ANS, les GRADeS ont créé et diffusé des messages de sensibilisation.

Ces campagnes vont être renforcées à l'occasion **du mois Européen de la cybersécurité en octobre**, afin de toucher plus largement l'écosystème sur les bonnes pratiques d'hygiène numérique et particulièrement les utilisateurs.

LES RECOMMANDATIONS

Dans le contexte actuel de l'utilisation croissante du numérique et comme il est d'usage au quotidien, l'importance des actions de prévention et de sensibilisation est rappelée. Une mobilisation collective et une vigilance permanente de l'ensemble des acteurs du numérique en santé est essentielle. Chacun doit poursuivre avec rigueur les procédures de signalement en cas de suspicion de fraude ou d'usage anormal d'une application mobile e-CPS.

La conduite à tenir est la suivante :

- Les **professionnels de santé** doivent contacter le **service client de l'ANS au 0 806 800 213** (appel gratuit + prix d'un appel) ou **monserviceclient.e-cps@esante.gouv.fr**, pour tout signalement ou demande d'assistance.
- Les **fournisseurs de services** et **autorités d'enregistrement** doivent adresser leurs signalements techniques directement à l'adresse dédiée : **psc.requisitions@esante.gouv.fr,**

L'ANS reste pleinement mobilisée pour garantir la sécurité des accès numériques en santé. Votre rôle est essentiel pour sensibiliser et accompagner les professionnels que vous représentez. Ensemble, nous devons renforcer la vigilance et maintenir la confiance dans les usages de la e-CPS.

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 08 06 80 02 13
esante.gouv.fr