

Direction des dispositifs médicaux et des dispositifs de diagnostic in vitro

Dossier suivi par Gwennaëlle EVEN

Tél. : +33 (0)55 87 37 21

E-mail : gwennaëlle.even@ansm.sante.fr

Saint-Denis, le 19/10/26

Objet : Incidents de cybersécurité concernant les dispositifs médicaux

Madame, Monsieur,

L'ANSM a été informée récemment de plusieurs alertes de sécurité consécutives à des incidents de cybersécurité susceptibles d'affecter le fonctionnement de dispositifs médicaux. Par ailleurs, l'actualité rapporte régulièrement des attaques de ce type visant divers équipements de santé.

Le dispositif médical constitue une cible privilégiée : l'impact sur le patient est direct, cet impact crée une pression maximale facilitant les demandes de rançon, et la connexion permanente de certains dispositifs au réseau de l'établissement de santé en fait une porte d'entrée vers son système d'information.

L'ANSM appelle l'attention des industriels du dispositif médical (DM) et du dispositif médical de diagnostic in vitro (DMDIV) sur les risques liés à la cybersécurité. La gestion de ces risques s'inscrit dans les obligations de sécurité et de performance qui incombent aux fabricants en application des règlements (UE) 2017/745 et 2017/746, et doit couvrir l'ensemble du cycle de vie du dispositif, de sa conception à l'anticipation de la réponse aux incidents.

Les familles de DM ou DMDIV suivantes sont d'ores et déjà identifiées comme pouvant être exposées à ce risque :

- Automates de diagnostic in vitro ;
- Pompes à perfusion ; Pompes à insuline ;
- Dispositifs cardiaques implantables et systèmes d'assistance cardiaque ;
- Moniteurs de patients ; Systèmes d'imagerie ; Échographes ;
- Endoscopie numérique ; Stérilisateurs ; Robotique chirurgicale ; Lithotripsie ; Radiothérapie ;
- Dispositifs médicaux utilisés à domicile et en télémedecine (ventilateurs, dialyse à domicile, télésurveillance) ;
- Logiciels dispositifs médicaux, dont les outils de diagnostic assistés par intelligence artificielle.

Cette liste n'est pas exhaustive.

Les fabricants sont invités à conduire, s'ils sont concernés, une analyse de vulnérabilité de leurs dispositifs, en portant une attention particulière aux équipements connectés, aux systèmes de surveillance et d'alarme, à la sécurisation des accès à distance ainsi qu'à la continuité de fonctionnement en cas de malveillance informatique. Il est également recommandé de vérifier l'adéquation des mesures de prévention et de gestion des actes de malveillance afin de garantir la détection rapide de toute attaque.

La page internet du site de l'ANSM <https://ansm.sante.fr/documents/reference/cybersecurite-des-dm-et-dmdiv> référence des documents pour accompagner les fabricants dans leur démarche de sécurisation des dispositifs médicaux dès les phases de conception.

Nous sommes également attentifs aux incidents qui pourraient concerner l'organisation des entreprises et la logistique.

Nous remercions les organisations professionnelles de bien vouloir sensibiliser leurs adhérents sur ce sujet et de leur rappeler que tout incident ou risque d'incident de cybersécurité mettant en cause un DM ou un DMDIV doit être signalé à l'ANSM dans le cadre des obligations de vigilance.

Dans le cas où vous seriez visé par une cyberattaque, vous pouvez vous référer aux consignes de l'État disponibles sur le site du CERT-FR : <https://cert.ssi.gouv.fr> (alerte en vigueur : CERTFR-2026-ALE-012).

Je vous prie de recevoir, Madame, Monsieur, mes salutations distinguées.

Direction des dispositifs médicaux et des dispositifs de diagnostic in vitro

Le directeur adjoint

Thierry
THOMAS

Signature numérique
de Thierry THOMAS

Date : 2026.10.19
08:36:45 +02'00'