VEDERE LABS

Exposition des dispositifs et systèmes médicaux à l'Internet

Sous-titre

Le 26 septembre 2022

1. Résumé

Le 12 septembre, le FBI a publié une notification du secteur privé intitulée « Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities » (Les dispositifs médicaux non corrigés et obsolètes offrent des possibilités de cyberattaques). La notification était axée sur le fait qu'un nombre croissant de vulnérabilités dans les dispositifs médicaux peuvent être exploitées par des acteurs de la menace pour « avoir un impact sur les fonctions opérationnelles des établissements de santé, la sécurité des patients, la confidentialité des données et l'intégrité des données ».

Cette notification intervient après la découverte, cette année, d'importantes vulnérabilités affectant des dispositifs médicaux tels que des pompes à perfusion, des systèmes de distribution de médicaments et des électrocardiographes, ainsi qu'une vague d'attaques par ransomware visant des organisations de soins de santé ces dernières années – certaines de ces attaques ayant rendu les dispositifs médicaux inutilisables.

Dans ce rapport, nous expliquons pourquoi les dispositifs médicaux sont vulnérables, nous allons au-delà des vulnérabilités pour fournir une image de l'exposition des dispositifs et systèmes médicaux sur l'Internet ouvert et nous discutons des recommandations d'atténuation pour les organismes de santé.

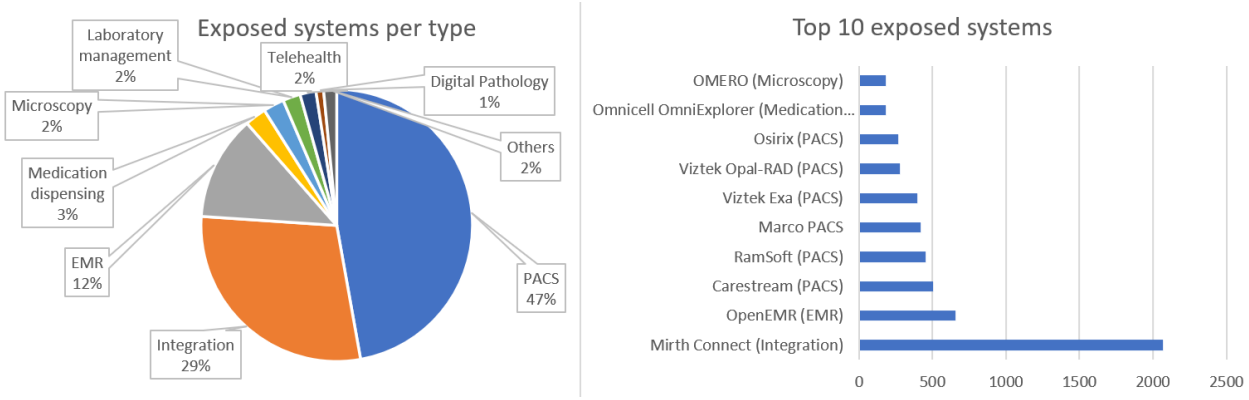
Les principales conclusions de ce rapport sont les suivantes :

- Nous avons trouvé plus de 7 000 systèmes médicaux exposés sur Internet, y compris des PACS, des moteurs d'intégration des soins de santé, des DME, des systèmes de distribution de médicaments et autres. Certains dispositifs médicaux, tels que les imprimantes d'images médicales, sont également directement exposés.
- Les États-Unis possèdent la grande majorité de ces systèmes exposés (58 % du total), suivis par l'Iran, l'Inde et le Brésil.
- Près de la moitié des systèmes exposés sont des PACS, qui s'appuient généralement sur le protocole DICOM pour le stockage et la récupération des images médicales. Si l'on considère les systèmes DICOM de manière spécifique, on observe 4 114 systèmes exposés, soit une augmentation de 14 % par rapport à l'année dernière.
- L'application d'une segmentation efficace du réseau est la mesure d'atténuation la plus importante compte tenu de nos constatations sur les systèmes exposés.

2. Une analyse des systèmes médicaux exposés à l'Internet

En utilisant une série d'empreintes de réseaux spécifiques de systèmes médicaux (accessibles à tous, y compris aux attaquants), nous avons interrogé le moteur de recherche Shodan et trouvé un total de 7 168 systèmes exposés. Plus des trois quarts des systèmes se trouvent sur le continent américain, les États-Unis en comptant à eux seuls 4 185 (58 % du total). La région Asie-Pacifique et Japon (APJ) arrive en deuxième position, principalement représentée par l'Inde (324 systèmes exposés) et l'Australie (146). L'Europe occupe la troisième position en tant que région, avec la majorité des systèmes exposés en Allemagne (128), au Royaume-Uni (75) et aux Pays-Bas (71). Et enfin, dans la région META (Moyen-Orient, Turquie et Afrique), le pays le plus représentatif est l'Iran, avec 427 systèmes exposés.

Les systèmes exposés sont divisés selon les types suivants.



Près de la moitié d'entre eux sont des PACS, utilisés pour le stockage et la visualisation d'images médicales reposant sur le protocole standard DICOM. La deuxième catégorie la plus populaire est celle des moteurs d'intégration des soins de santé, utilisés pour normaliser les flux de données entre des systèmes distincts, tels que les données cliniques, financières et opérationnelles. Ces moteurs utilisent souvent le protocole standard HL7. La troisième catégorie est celle des systèmes de dossiers médicaux électroniques (DME) utilisés pour gérer les données de santé des patients. Une catégorie intéressante et surprenante du top 10 est celle des systèmes de distribution de médicaments, généralement utilisés dans les pharmacies d'hôpitaux.

En examinant uniquement les 10 systèmes les plus exposés, nous avons constaté que sur les 5 405 systèmes, 882 (16 %) présentaient au moins une vulnérabilité identifiée par Shodan. Pour certains systèmes, le taux de vulnérabilité était beaucoup plus élevé. Pour Opal-RAD PACS, il est de 69 %, pour Carestream PACS, il est de 50 % et pour OpenEMR, il est de 31 %. Il est également important de noter que de nombreux autres systèmes peuvent présenter des vulnérabilités qui ne sont pas automatiquement identifiées par le moteur de recherche.

Les PACS étant le type de système exposé le plus courant, nous avons décidé de les examiner de plus près. Comme mentionné ci-dessus, les systèmes PACS utilisent généralement le protocole DICOM. Nous avons donc étendu notre recherche pour trouver des systèmes plus exposés en utilisant la requête « DICOM Server Response » (réponse du serveur DICOM), qui a donné 4 114 nouveaux résultats. Les dispositifs utilisant DICOM exposent le nom (ou un identifiant) de l'application serveur sur la bannière saisie par Shodan. L'un des serveurs les plus populaires trouvés en ligne utilise le kit d'outils DICOM OFFIS, dont une série de vulnérabilités a été divulguée pas plus tard qu'en juin.

3. Recommandations d'atténuation

La notification du FBI propose cinq catégories de mesures d'atténuation pour les dispositifs médicaux vulnérables :

- Exécuter la protection des points d'extrémité, comme l'antivirus et l'EDR, sur les dispositifs qui prennent en charge ces technologies.
- Utiliser des mots de passe complexes et uniques par dispositif et limiter le nombre de tentatives de connexion.
- Tenir un inventaire des dispositifs médicaux et l'utiliser pour l'évaluation des risques.
- Suivre les avis de sécurité des fournisseurs et effectuer des analyses de vulnérabilité sur les dispositifs médicaux.
- Mettre en place une formation à la sécurité pour les employés afin qu'ils puissent identifier et signaler des problèmes tels que les menaces internes, le phishing et l'ingénierie sociale.

La notification encourage également à « prendre d'autres mesures d'atténuation, telles que l'isolement du dispositif du réseau ou l'audit des activités réseau du dispositif ». Pour des directives plus détaillées sur la mise en œuvre de la segmentation pour des types de dispositifs spécifiques tels que les PACS, les DME et les pompes à perfusion, voir les publications d'orientation sur la sécurité du NIST. Pour des conseils généraux sur l'évaluation des risques des dispositifs médicaux, voir le récent NIST SP 800-66.

La segmentation du réseau est extrêmement importante compte tenu de nos constatations sur les systèmes exposés. Les recommandations du FBI, en particulier la segmentation et la surveillance du réseau, devraient s'appliquer non seulement aux dispositifs médicaux, mais aussi à chaque appareil du réseau de votre organisation. Comme nous l'avons montré dans des articles précédents et comme le Health Sector Cybersecurity Coordination Center (HC3, centre de coordination de la cybersécurité pour le secteur de la santé) l'a récemment évoqué, les acteurs de la menace peuvent tirer parti de ces autres types de dispositifs pour accéder aux organisations de soins de santé ou les affecter.

Pour plus d'informations et d'analyses techniques, lisez ici le rapport complet.