

VULNERABILITES DE PRODUITS DU SECTEUR SANTE : RETOUR D'EXPERIENCE DU CERT SANTE ET DU CERT-FR

Le CERT Santé et le CERT-FR assurent le traitement des vulnérabilités qui leur sont signalées par des tiers. A ce titre, ils accompagnent les éditeurs affectés dans la conception et le suivi de plan d'action incluant le développement de correctifs et la communication vers leurs utilisateurs.

Dans le cadre de ces activités, ainsi qu'à l'occasion des accompagnements réalisés lors d'incidents de sécurité, la présence de vulnérabilités critiques facilement exploitables depuis Internet a pu être observée dans plusieurs solutions numériques déployées au sein des structures de santé. Un récent sondage de l'Agence du Numérique en Santé auprès d'établissements de santé permet d'illustrer ces constats :

- 82% des répondants ont eu connaissance de vulnérabilités sur leur système lors des douze derniers mois ;
- 74% des répondants ont été confrontés à des éditeurs qui tardent ou refusent de corriger des vulnérabilités ;
- 90% des répondants n'ont pas de canal formalisé pour remonter les vulnérabilités aux éditeurs.

Dans plusieurs cas, ces vulnérabilités peuvent être identifiées puis exploitées avec un faible niveau de compétences techniques. Leur exploitation peut avoir un impact direct potentiel sur la confidentialité des données de santé, mais également sur la continuité des soins et la sécurité des patients. En outre, le déploiement important de certains logiciels de santé expose simultanément un grand nombre de structures de santé à une même vulnérabilité, augmentant significativement le risque d'attaque à large échelle.

En dépit d'une transparence et d'un engagement croissant de nombreux éditeurs, les pratiques observées restent insuffisantes au regard du niveau de menace pesant sur le secteur de la santé. Cette menace continue de croître, avec une augmentation du nombre d'incidents d'origine malveillante traités par le CERT Santé passé de 328 en 2024 à 400 en 2025 (+22 %). Elle se trouve par ailleurs amplifiée par les technologies d'intelligence artificielle.

Compte tenu des risques importants que cette situation fait peser sur les établissements de santé, le CERT Santé et le CERT-FR proposent dans ce rapport un retour d'expérience. Fondé sur des cas réels anonymisés pour ne pas mettre en évidence un acteur en particulier, il est destiné à sensibiliser les acteurs du secteur aux risques et à leur responsabilité en matière de sécurité informatique.

En coordination avec le CERT Santé, le CERT-FR émettra lorsque nécessaire des avis de sécurité destinés à informer les utilisateurs des vulnérabilités affectant les produits concernés et à proposer des mesures permettant de se prémunir de leur exploitation (<https://www.cert.ssi.gouv.fr/avis/>).

VULNERABILITES ET MAUVAISES PRATIQUES OBSERVEES

Délais de correction et communication inadaptés

La gestion satisfaisante de vulnérabilités significatives implique non seulement leur correction rapide, mais également une communication adaptée auprès des clients et utilisateurs afin qu'ils connaissent les risques auxquels ils sont exposés et soient incités à appliquer les correctifs disponibles.

Pour 4 éditeurs importants du secteur santé, le traitement de vulnérabilités actuellement en cours dure depuis plus d'un an. Dans l'un des cas, le déploiement du dernier correctif, pour une vulnérabilité de criticité moyenne, a été planifié 5 ans après son signalement.

Plusieurs facteurs contribuent à ces délais :

- Correctifs de sécurité systématiquement intégrés à des évolutions fonctionnelles : cette pratique impose d'attendre la sortie d'une nouvelle version fonctionnelle, souvent très espacée dans le temps, pour déployer un correctif. De plus, parce que ces évolutions fonctionnelles nécessitent des changements de pratique, ou qu'elles sont payantes, les clients peuvent en retarder le déploiement voire y renoncer, et donc rester vulnérables ;
- Support d'un grand nombre de versions et d'environnements : dans ces cas, s'expliquant souvent par un historique d'adaptation à différentes spécificités clients, l'éditeur doit développer et tester les correctifs dans un très grand nombre de contextes, ce qui multiplie l'effort nécessaire et les risques d'effet de bord et retarde le déploiement. Le déploiement étant par ailleurs souvent assuré directement par l'éditeur, la durée d'exposition des services vulnérables s'en trouve encore allongée ;
- Communication limitée : l'absence de canal prédéfini pour avertir les clients de vulnérabilités et des correctifs à appliquer limite leur connaissance des risques encourus et, par conséquent, leur motivation pour appliquer les mises à jour ;
- Nécessité de refonte du code : la prise en compte tardive de la sécurité dans une base de code conséquente nécessite une refonte coûteuse en ressources et en temps ;
- Contraintes réglementaires : la réglementation spécifique aux dispositifs médicaux et leur marquage CE complexifie le développement et le déploiement de correctifs dans certains cas. Le respect des bonnes pratiques usuelles en matière de sécurité, et en particulier celles imposées par le Cyber Resilience Act (cf. Renforcement du cadre réglementaire) est indispensable pour revenir à une situation acceptable en matière de risques.

Gestion des secrets insuffisante

Des produits d'au moins 3 éditeurs majeurs ont fait l'objet d'un signalement portant sur une mauvaise gestion des secrets permettant de protéger l'infrastructure ou les données, et notamment :

- Secrets accessibles à tout utilisateur par simple saisie d'une adresse (URL) dans le navigateur Web. Dans un cas, il était ainsi possible de récupérer facilement le mot de passe du serveur hébergeant le service ;
- Répertoire .git accessible sur le site Internet, permettant la récupération du code source de l'application contenant des secrets ;
- Identifiant et mot de passe du compte administrateur du logiciel accessibles dans le code de l'application ;
- Identifiant et mot de passe de télémaintenance gardés à leur valeur par défaut sur différents sites.

Outre la compromission du service affecté, et donc des données de santé qu'il traite, ces faiblesses, corrigées depuis dans les cas signalés, peuvent permettre une latéralisation de l'attaquant sur les environnements des clients. Ainsi, dans un cas, la récupération et l'utilisation des identifiants utilisateur dans le code, associées à l'autorisation d'accès au serveur au sein de dizaines d'établissements de santé, auraient pu faciliter la latéralisation sur ces établissements et l'accès aux données de milliers de patients.

Ces vulnérabilités résultent d'une protection insuffisante des secrets tout au long du cycle de développement et d'utilisation par les applications concernées. Il convient de rappeler en particulier que le cycle de développement doit identifier, protéger et distribuer de manière adéquate les secrets de différentes natures et que la configuration des serveurs doit limiter l'accès aux seules ressources nécessaires. Toute défaillance détectée dans cette gestion doit occasionner le remplacement des secrets concernés sur toutes les instances qui les utilisent.

Manque de contrôles et d'assainissement des entrées utilisateurs

Une partie des vulnérabilités signalées concerne des possibilités d'injection de code par les utilisateurs, telles que des XSS (injection de code JavaScript dans le navigateur des utilisateurs) ou SQLi (injection de code SQL côté serveur). Les conséquences possibles vont du vol d'une session utilisateur à la prise de contrôle complète de l'application, voire du serveur, et de ses données.

L'échange avec les éditeurs en vue de la correction des vulnérabilités a plusieurs fois mis en évidence qu'une même vulnérabilité était présente à de multiples endroits de l'application. Pour l'un d'eux, un contre-audit a ainsi relevé que le code de l'application était toujours vulnérable à plusieurs XSS plus d'un an après le correctif initial.

Cette situation s'explique selon les cas par un manque de prise en compte systématique de la sécurité ou par le développement en interne des fonctions de sécurité. A ce titre, deux principes fondamentaux doivent être rappelés :

- Toutes les données (champ de formulaire, en-tête HTTP, paramètre d'URL, etc.) provenant d'un utilisateur peuvent être manipulées et détournées à des fins malveillantes.

- Il est donc indispensable de contrôler systématiquement toute entrée utilisateur et de s'assurer qu'elle ne peut être interprétée d'une manière non souhaitée par l'application ;
- Des briques logicielles éprouvées, maintenues et documentées doivent être utilisées pour le contrôle et l'assainissement des données. Les développements internes de telles fonctions, complexes et critiques, sont à proscrire.

Ce dernier principe s'applique également à toutes les fonctions de sécurité : authentification (incluant la modification d'email ou la réinitialisation de mot de passe), autorisation (cf. Contrôle d'accès déficient), stockage des mots de passe, chiffrement, etc. ¹

Il est enfin à noter que dans plusieurs cas l'utilisation de pare-feu applicatif Web (WAF) a été conseillée par l'éditeur pour réduire le risque d'exploitation des vulnérabilités. Si cette solution, parfois vendue par l'éditeur lui-même, peut contribuer à la sécurité, elle ne saurait remplacer l'implémentation des mesures adaptées dans les applications.

Exposition non sécurisée sur Internet

Le CERT Santé et le CERT-FR ont identifié de nombreuses instances d'un même logiciel de santé, exposées sur Internet, accessibles sans authentification.

Cette pratique expose les machines concernées à des accès illégitimes pouvant ne pas être détectés par des utilisateurs légitimes, avec un risque important d'accès à des données personnelles et de santé, voire de prise de contrôle des systèmes concernés. Des attaquants peuvent par ailleurs en tirer parti de manière opportuniste, la détection de ce type de vulnérabilité étant accessible avec des moyens et des compétences limitées. Toute machine exposée de la sorte a donc un risque très important d'être prise pour cible.

Contacté à ce sujet, l'éditeur de ce logiciel a indiqué avoir engagé des actions de remédiation notamment en sollicitant ses clients afin de fermer les accès distants identifiés, en particulier sur les serveurs exposés. Selon l'éditeur, dans certains cas, les accès VNC ont été fermés, tandis que dans d'autres les clients ont choisi de maintenir ces accès. Pour ces derniers, une décharge de responsabilité a été signée.

Comme le CERT Santé et le CERT-FR l'ont indiqué à l'éditeur, le besoin d'accès distants peut être légitime et, plutôt que d'y renoncer ou d'imposer une solution complexe ou coûteuse, la configuration d'une authentification robuste, native et simple sur ce type d'outils, doit être mise en place systématiquement. D'autres mesures plus robustes (MFA, VPN, etc.) peuvent ensuite être considérées pour renforcer la sécurité.

Les CERT et l'éditeur poursuivent leur coopération pour réaliser les actions nécessaires à la réduction de ce risque.

¹ Dans le cas de logiciel libre, des principes pour leur sélection sont définis ici : <https://messervices.cyber.gouv.fr/guides/selection-dun-logiciel-libre>

Contrôle d'accès déficient

Plusieurs logiciels de santé ont fait l'objet de signalements de tiers faisant état d'une possibilité pour les utilisateurs d'accéder de manière indue aux données d'autres utilisateurs. Ce manque de cloisonnement, souvent très simple à exploiter, permet à tout utilisateur disposant initialement d'un accès légitime (praticien, mais aussi parfois simple patient) de collecter illégitimement des données de santé de très nombreux patients.

Ce type de vulnérabilité est particulièrement exploité actuellement sur des solutions numériques de santé, notamment en mode SaaS.

Dans les cas observés, les attaquants commencent généralement par compromettre un compte de professionnel de santé (par hameçonnage ou utilisation de mots de passe compromis). Une fois connectés avec un compte légitime, ils exploitent ensuite les faiblesses de contrôle d'accès pour élargir progressivement leur périmètre en accédant à des données d'autres utilisateurs ou établissements. Ce mode opératoire permet des accès massifs à des données de santé, tout en restant difficilement détectable.

Cette vulnérabilité résulte généralement de pratiques de développement insuffisantes en matière de sécurité. Dans certains cas cependant, ce comportement a été développé en connaissance de cause pour répondre à la demande de certains clients de faciliter la coopération sur des dossiers.

Le CERT-FR et le CERT Santé émettent des recommandations aux éditeurs concernant le développement et le déploiement de correctifs adaptés en rappelant quelques principes fondamentaux :

- Le contrôle d'accès, c'est-à-dire la limitation de chaque utilisateur aux seules actions et données légitimes, doit être systématiquement implémenté selon le principe de moindre privilège interdisant toute action non explicitement autorisée ;
- Les demandes d'utilisateurs et de clients ne doivent pas être satisfaites aux dépens de la sécurité, par exemple par une ouverture massive de droits d'accès, mais par des solutions adaptées au juste besoin.

Cette même logique s'applique aux flux réseau, fréquemment autorisés par défaut et exposant par conséquent des services internes sur Internet. Dans ces deux cas la mise en œuvre de mécanismes de détection et d'alerte portant sur les accès inhabituels ou massifs à des données sensibles est recommandée afin d'identifier d'éventuelles exfiltrations de données.

RENFORCEMENT DU CADRE REGLEMENTAIRE

Le règlement (UE) 2024/2847 sur la cyber résilience (Cyber Resilience Act ou CRA) définit les exigences de cybersécurité que doivent satisfaire les produits comportant des éléments numériques pour être mis à disposition sur le marché européen. Il entrera pleinement en application le 11 décembre 2027², et

² L'article 14, imposant aux éditeurs de déclarer les vulnérabilités activement exploitées et les incidents graves affectant la sécurité des produits sur une plateforme unique européenne s'applique d'ores et déjà depuis le 11 septembre 2026.

s'appliquera également aux logiciels et matériels du secteur santé, à l'exception des dispositifs médicaux et dispositifs médicaux de diagnostic in vitro qui font l'objet d'une réglementation spécifique.³

En particulier, [l'annexe 1 du Cyber Resilience Act](#) définit en deux pages les exigences relatives aux produits et à la gestion des vulnérabilités, et notamment :

- Mettre à disposition le produit avec une configuration de sécurité par défaut ;
- Concevoir les produits pour que leurs vulnérabilités puissent être corrigées par des mises à jour de sécurité. Lorsque cela est techniquement possible, de nouvelles mises à jour de sécurité sont fournies séparément des mises à jour de fonctionnalités ;
- Assurer la protection contre les accès non autorisés par des mécanismes de contrôle appropriés ;
- Gérer et corriger sans retard les vulnérabilités ;
- Soumettre régulièrement les produits à des tests et examens de sécurité efficaces ;
- Dès la publication d'une mise à jour de sécurité, communiquer sur les vulnérabilités corrigées ;
- Mettre en place et appliquer une politique de divulgation coordonnée des vulnérabilités ;
- Prévoir des mécanismes de distribution sécurisée des mises à jour ;
- Veiller à diffuser sans retard les correctifs ou mises à jour de sécurité.

En France, il est prévu que l'Agence Nationale des Fréquences (ANFR) assure le rôle d'autorité de surveillance du marché au titre du CRA. Ainsi, l'ANFR sera chargée de contrôler le marché et pourra mettre en place les sanctions prévues par le règlement en cas de manquement, incluant une amende administrative pouvant atteindre 15 M€ ou 2,5% du chiffre d'affaires annuel mondial, rappel et retrait du marché. Le CERT Santé et le CERT-FR pourront signaler à l'ANFR tout élément susceptible de constituer un manquement d'un éditeur à ses obligations constaté dans le cadre de leurs missions de réponse à incidents et de traitement des signalements de vulnérabilités.

³ Règlement (UE) 2017/745 relatif aux dispositifs médicaux et règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro.