Nom Laurent Calatayud
Entité HC WEA FRA SV CS SO TSC AX&XP&US

Téléphone 0820 80 75 69
email laurent.calatayud@siemens-healthineers.com

**N/réf**. **AX047/17/S**

Date Juillet 2017

Siemens Healthcare S.A.S, HC WEA FRA SV CS SO TSC AX&XP&US,
40, avenue des Fruitiers, SISLEY, 93200 Saint-Denis

A l'attention du Directeur de l'Etablissement,
du correspondant local de matériovigilance

Lettre recommandée avec AR n°

# IMPORTANT : Lettre de sécurité

## Informations relatives sur une potentielle vulnérabilité dans le système d'exploitation Microsoft Windows des systèmes Artis, X Workplace, Sensis et Arcadis

N° Installation :
Modification: **AX047/17/S**

Cher client, Chère Cliente

Le présent courrier a pour objet de vous informer d'un problème de sécurité éventuel pouvant toucher les patients.

**Quel est le dysfonctionnement et à quel moment se produit-il ?**

Les systèmes Artis, X-Workplace, Sensis et Arcadis fonctionnent sur le système d'exploitation Windows XP ou Windows 7. Une faille dans ces systèmes d'exploitation est à l'origine d'un danger sérieux.
Un logiciel malveillant, connu sous le nom de "WannaCry", s'attaque de manière ciblée à cette faille, envahit les systèmes vulnérables et corrompt les données sur ces systèmes en les cryptant.

**Quelle est l'incidence sur le fonctionnement du système et quels sont les risques potentiels ?**

Le logiciel malveillant crypte des données se trouvant sur les systèmes attaqués. L'encryptage de parties du système Artis, de la station X-Workplace, de Sensis ou du système Arcadis peut provoquer un dysfonctionnement et conduire à une situation exigeant l'arrêt ou le redémarrage d'un traitement clinique voire son transfert sur un système en état de marche.

Indirectement, les données acquises précédemment peuvent aussi être perdues.

**Quelle action pouvez-vous prendre ?**

L'exploitation d'une telle vulnérabilité dépend de la configuration réelle et de l'environnement de déploiement de chaque produit. Selon Microsoft, ce logiciel de rançonnage se propage par pièces jointes, des liens dans des courriers électroniques hameçons, sur des sites malveillants (« systèmes zéro infection ») ou via des systèmes infectés qui exploitent une vulnérabilité dans un composant Windows utilisé dans un contexte de partage de fichiers ou accessibles sur le même réseau. Certains détails sont expliqués sur la page Microsoft suivante : https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

Nous souhaiterions souligner que ni l'usage de courriers électroniques client ni l'utilisation d'internet font partie de l'usage prévu pour la plupart des types de produits.

Recommandations

Les systèmes concernés par cette lettre et détaillés dans le paragraphe suivant sont obsolètes soit concernant la partie matériel (hardware) soit concernant la partie logiciel (software).

Pour les systèmes suivants aucun Patch Microsoft ne peut être déployé.

**Arcadis**

| | |
|---|---|
| Arcadis Varic | (P/N 8080017) |
| Arcadis Orbic | (P/N 8081080) |
| Arcadis Avantic | (P/N 10048590) |
| Arcadis Varic Gen2 | (P/N 10143406) antérieur au n° de série15000 |
| Arcadis Orbic Gen2 | (P/N 10143407) antérieur au n°de série 23000 |
| Arcadis Avantic Gen2 | (P/N 10143408) antérieur au n°de série 33000 |

**syngo X-WP**

| | |
|---|---|
| X-Leonardo | VA70, VA71, VA72, VB11A/B, VB11M |

La vulnérabilité des produits ci-dessus concerne les ports de réseau : 139/tcp, 445/tcp or 3389/tcp.
Leur exposition à être exploités dépend des mesures de sécurité dans le réseau.
Afin de protéger un produit vulnérable d'une exploitation malveillante, il devra être isolé de tout système potentiellement infecté dans son segment de réseau respectif. (par ex : produit déployé dans un segment de réseau séparé par un firewall bloquant l'accès aux ports de réseau 139/tcp, 445/tcp or 3389/tcp).

Si la solution, ci-dessus, ne peut pas être mise en œuvre, nous vous recommandons les dispositions suivantes :

- Si la sécurité du patient et de son traitement ne sont pas en danger, déconnectez le produit non-infecté du réseau et utilisez-le en mode autonome.
- Pour les systèmes suivants nous recommandons de mettre à jour les logiciels des systèmes obsolètes par une version pour laquelle un Patch Microsoft peut être déployé :

**Artis**

| | | |
|---|---|---|
| AXIOM Artis | VB22N, VB23D/F/G/H/J | -> Mettre à jour à VB23P |
| AXIOM Artis | VB30C/E, VB31E/F, VB35A | -> Mette à jour à VB35E |
| Artis zee | VC13A/B, VC13D/E, VC14B/D/E/G | -> Mettre à jour à VC14J |
| Artis zee | VC21A | -> Mettre à jour à VC21C |
| Artis One | VA10B, VA10C | -> Mettre à jour VA10D |

**Syngo X-WP**

| | | |
|---|---|---|
| syngo X-WP | VB13E | -> Mettre à jour à VB13F |
| syngo X-WP | VB14A, VB14B | -> Mettre à jour à VB14C |
| syngo X-WP | VB12B, VB15C | -> Mettre à jour à VB15D |
| syngo X-WP | VB20B, VB20C | -> Mettre à jour à VB20D |
| syngo X-WP | VB21B | -> Mettre à jour à VB21C |
| syngo X-WP | VC10C | -> Mettre à jour à VC10D |

**Sensis**

| | | |
|---|---|---|
| Sensis | VC03A/B/C/D | -> Mettre à jour à VC03G ou plus tard |
| Sensis | VC10B/C, VC11A/B/C | -> Mettre à jour à VC11D ou plus tard |
| Sensis | VC12A | ->Mettre à jour à VC12C ou plus tard |
| Sensis | VC12K | -> Mettre à jour à VC12L ou plus tard |

De plus, Siemens Healthineers recommande de vous assurer de la mise en œuvre de sauvegardes et deet procédures de restauration de système appropriés.

**Comment le problème a-t-il été décelé ?**

La menace a été identifiée lorsque l'infection de certains équipements industriels privés de santé a été signalée. Une possible vulnérabilité des systèmes Artis, Sensi et Arcadis doit être envisagée.

**Quels sont les risques pour les patients déjà examinés ou traités avec ce système ?**

Dans le cas présent, nous ne jugeons pas nécessaire de réexaminer les patients.
Il s'agit d'un défaut possible n'ayant pas d'influence sur le traitement des patients.

Nous vous remercions de votre coopération au regard de cette lettre de sécurité et vous invitons à la transmettre immédiatement à votre personnel concerné au sein de votre établissement et lui donner des instructions en conséquence. Merci également de transmettre les présentes informations de sécurité aux autres établissements qui pourraient être visés par cette action.

Si vous avez vendu cet équipement et qu'il n'est plus en votre possession, nous vous invitons à transmettre cette lettre de sécurité à son nouveau propriétaire. Merci également de nous communiquer les coordonnées de ce dernier.
L'Agence Nationale de Sécurité du Médicament et des produits de santé a été informée de cette communication.

Pour toute question relative à ce courrier, vous pouvez également contacter le centre de support client Siemens Healthcare SAS France au 0 820 80 75 69 et indiquer votre n° d'installation.

Veuillez agréer, Cher Client, Chère Cliente, nos respectueuses salutations.

Signé.

**Jérome Chedin**
Ingénieur support technique

Signé.

**Nathalie DUCROCQ**
Directeur Affaires Réglementaires, Qualité et HSE