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. **AX037/17/S**

Date Juin 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 à une action corrective sur les systèmes Artis, X-Workplace, Sensis et Arcadis pour éliminer une faille dans le système d'exploitation Microsoft Windows

N° Installation :
Modification: **AX037/17/S**

Cher client, Chère Cliente

Le présent courrier a pour objet de vous informer d'une action corrective destinée à éviter une situation potentiellement dangereuse pour les patients.

Quel est le problème à l'origine de cette action corrective et quand survient-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 quel est le risque potentiel ?

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

Les données acquises précédemment peuvent aussi être perdues (effet indirect).

Quelles mesures seront prises ?

Le logiciel sera corrigé sur les systèmes concernés avec une mise à jour ayant pour objectif d'éliminer la faille dans Microsoft Windows. Les mises à jour de terrain suivantes ont été définies :

AX038/17/S –	ARTIS:	OS HOTFIX-UPDATE WIN XP SMB VULNERABILITY
AX039/17/S –	ARTIS:	OS HOTFIX-UPDATE WIN 7 SMB VULNERABILITY
AX041/17/S –	X-WP:	OS HOTFIX UPDATE WIN XP SMB VULNERABILITY
AX042/17/S –	X-WP:	OS HOTFIX UPDATE WIN 7 SMB VULNERABILITY
AX046/17/S –	SENSIS:	OS HOTFIX UPDATE SMB VULNERABILITY
AX043/17/S -	ARCADIS:	OS HOTFIX-UPDATE WIN XP SMB

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

La menace a été identifiée par la signalisation de l'infection de certains équipements privés, industriels et médicaux. La vulnérabilité des systèmes Artis, X-Workplace, Sensis et Arcadis ne peut pas être exclue. À ce jour, un seul cas isolé d'infection d'un système Sensis nous a été rapporté.

Quelle est l'efficacité des mesures correctives ?

La mise à jour du logiciel éliminera la cause du problème et offrira une protection contre les attaques par le logiciel de rançon "WannaCry" ou tout autre logiciel malveillant utilisant les failles de MS Windows ciblées par ce correctif.

Comment l'action corrective sera-t-elle mise en œuvre ?

La mise à jour logicielle sera réalisée à distance. Si une telle mise à jour à distance n'est pas possible, notre service technique vous contactera sous peu pour convenir d'une date d'intervention. N'hésitez pas à prendre contact avec lui si vous souhaitez obtenir un rendez-vous plus rapidement. Ce courrier sera transmis à tous les clients concernés sous la référence AX037/17/S.

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.
Laurent CALATAYUD
Responsable d'Activité Radiologie

Signé.
Nathalie DUCROCQ
Directeur Affaires Réglementaires, Qualité et EHS