ADVISORY : DIVERSES VULNÉRABILITES DANS LES APPAREILS D'IMAGERIE MOLÉCULAIRE DE SIEMENS (SYSTÈME PET/CT/SPECT)

Référence : CERT.be Advisory #2017-005
Version : 1.0
Logiciel affecté : l'ensemble des versions des systèmes PET/CT/SPECT de Siemens basé sur Windows 7, l'ensemble des postes de travail SPECT Windows 7 / Sybmia.net & Mobilett Mira Max: Toutes les version avant VE10S without XP009/17/S
Type : le code peut être exécuté avec les droits de l'utilisateur local

Sources

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-822184.pdf
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-131263.pdf

Risques

L'exploitation fructueuse de ces vulnérabilités offre la possibilité au pirate d'exécuter du code avec les droits de l'utilisateur local, ce qui lui donnerait accès complet au système (i.e. Voler ou modifier des informations sur les patients, Modifier les configurations de la machine, etc…).

Ces vulnérabilités ont obtenu un résultat CVSS v3 de 9.8 sur 10. L'impact de ces vulnérabilités est fonction de nombre de facteurs propres à chaque organisation.

Résumé

Siemens a identifié plusieurs vulnérabilités dans les produits d'imagerie moléculaire de Siemens qui sont basés sur Windows 7. De plus, Siemens a aussi communiqué que de multiples vulnérabilités ont été trouvé dans leurs machines Mobilett Mira Max – machines à rayon-X portables.

Ces vulnérabilités peuvent être exploitées à distance. Des exploits pour ces vulnérabilités sont disponibles au public et leur exécution ne requière que peu d'efforts.

Affected Products:

- Siemens PET/CT Systems: Toutes les versions basées sur Windows 7
- Siemens SPECT/CT Systems: Toutes les versions basées sur Windows 7
- Siemens SPECT Systems: Toutes les versions basées sur Windows 7
- Siemens SPECT Workplaces / Symbia.net: Toutes les versions basées sur Windows 7

- Mobilett Mira Max: Toutes les versions avant VE10S non-compris XP009/17/S

Il est a noté que le système d'exploitation utilisé par une machine est affiché au lancement de ladite machine.

Pour les systèmes CT/PET/SPECT basés sur Windows 7 :

Vulnérabilité CVE-2015-1635 :

Un pirate externe non authentifié peut exécuter du code qu'il contrôle en envoyant des demandes HTTP spécialement formulées au serveur web Microsoft (port 80 / tcp et port 443 / tcp) des systèmes affectés.

Vulnérabilité CVE-2015-1497 :

Un pirate externe non authentifié peut exécuter du code qu'il contrôle en envoyant une demande HTTP spécialement formulée au service clientèle d'automatisation d'HP sur le port 3465 / tcp des appareils affectés.

Vulnérabilité CVE-2015-7860 / 7861 :

Un pirate externe non authentifié peut exécuter du code qu'il contrôle en envoyant une demande HTTP spécialement formulée au service clientèle d'automatisation d'HP des appareils affectés.

Pour les machines Mobilett Mira Max :

Vulnerability CVE-2017-0143 / 0144 / 0145 / 0146 / 0147 / 0148:

Un pirate externe non authentifié peut exécuter du code qu'il contrôle en envoyant une demande spécialement formulée au server SMBv1 de la machine.

Actions préconisées

Pour les machines CT/PET/SPECT tournant sous Windows 7 :

Siemens œuvre au développement de mises à jour pour les produits affectés et conseille de sécuriser l'accès au réseau des dispositifs d'imagerie moléculaire grâce à des mesures adéquates.

Siemens préconise l'utilisation de ces appareils dans un segment de réseau distinct (*dedicated*) dans un environnement IT suffisamment protégé jusqu'à ce que ces mises à jour soient disponibles.

Pour les machines Mobilett Mira Max avant VE10S non-compris XP009/17/S :

Siemens fournit la mise à jour XP009/17/S pour les versions supportées de Mobilett Mira Max avant VE10S.

La mise à jour sera directement disponible pour les clients qui possède le support à distance de Siemens. Si le support à distance n'est pas disponible ou si vous avez des questions concernant la mise à jour, veuillez contacter le support clientèle de Siemens.

En attendant que la mise à jour soit disponible et pour les produits en fin de maintenance, Siemens recommande d'isoler du réseau les machines affectées qui écoutent sur les ports réseaux 139/TCP, 445/TCP ou 3389/TCP en bloquant le trafic sur ces ports au moyen d'un firewall par exemple.

Si cela s'avère impossible, Siemens émet les recommandations suivantes :

- Si la sécurité du patient et le traitement ne sont pas menacés, retirez l'appareil du réseau et utilisez-le en fonctionnement autonome.

- Reconnectez le produit au réseau uniquement après avoir installé la mise à jour sur le système. Siemens a la possibilité de mettre à jour bien plus rapidement des systèmes supportant le *Remote Update Handling (RUH)* qu'en procédant à une intervention sur place. Il est recommandé aux clients qui possèdent des dispositifs RUH d'expliquer au service clientèle de Siemens la situation quant à la disponibilité de correctifs ainsi qu'à l'existence de risques qui persistent dans le réseau. Ils doivent ensuite à nouveau connecter leurs systèmes afin de recevoir sans délai les mises à jour par l'intermédiaire du *Remote Update Handling*. Ainsi, les mises à jour sont apportées facilement et rapidement, et la restauration de systèmes d'exploitation est facilitée.

Siemens prodigue également les conseils suivants :

- Assurez-vous que vous disposez des sauvegardes et des procédures de restauration système adéquates.

- Pour obtenir des informations spécifiques concernant des mises à jour et des solutions, vous pouvez prendre contact avec votre service clientèle engineer local Siemens ou avec un centre régional d'assistance.

CERT.be recommande par ailleurs aux organisations de prendre des mesures défensives en vue de minimaliser le risque. Citons les suivantes :

- Minimalisez l'accès au réseau de l'ensemble des appareils et/ou systèmes médicaux et veillez à ce qu'ils ne soient pas disponibles depuis Internet.

- Placez tous les appareils médicaux et externes derrière des pare-feu et isolez-les du réseau de l'entreprise.

- Lorsqu'un accès externe est requis, recourez à des méthodes sécurisées telles que les réseaux privés virtuels (VPN). Il convient également de distinguer le risque dans les VPN qui peuvent aussi contenir des vulnérabilités et qui doivent être mis à jour grâce à la dernière version. Sachez également qu'un réseau VPN présente le même degré de sécurité que les appareils qui y sont connectés.

Références

Vous trouverez de plus amples informations concernant ces failles de sécurité ainsi que des instructions détaillées d'atténuation dans le « Siemens Security Advisory SSA-814457 / 131263 » à l'emplacement suivant :

http://www.siemens.com/cert/advisories