Lettre pour les appareils munis de commande CX2020

Note importante sur les stérilisateurs Miele PS5XXX

Madame, Monsieur..... (Responsable stérilisation centrale / responsable de laboratoire / propriétaire de cabinet, ajouter le destinataire),

Selon nos documents, vous utilisez dans vos locaux, des stérilisateurs de type PS5 XXXX de Miele. Ces appareils sont équipés d'une interface réseau qui permet de les connecter à un réseau local à des fins de traçabilité des charges.

Par la présente lettre, nous souhaitons vous informer que nous avons eu connaissance dans le cadre de nos contrôles de sécurité réguliers de **failles du système d'exploitation Microsoft utilisé dans l'appareil**.

Il s'agit des failles suivantes :

Application concernée	Information sur la faille	CVE
Microsoft Windows protocole SMBv1	Le service Microsoft SMBv1 (port 445) présente diverses failles qui auraient pour conséquence lors de l'exploitation, la divulgation d'informations, l'arrêt brutal du système ou l'exécution d'un code à distance. [1]	CVE-2017-0267 CVE-2017-0268 CVE-2017-0270 CVE-2017-0271 CVE-2017-0274 CVE-2017-0275 CVE-2017-0276 CVE-2017-0269 CVE-2017-0273 CVE-2017-0280 CVE-2017-0272 CVE-2017-0277 CVE-2017-0278 CVE-2017-0279
Microsoft Windows serveur SMB	MS17-010 [2]	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148
Microsoft HTTP.sys	MS15-034 [3]	CVE-2015-1635
Microsoft Windows service RDP (port 3389)	MS14-066 [4]	CVE-2014-6321

Risques possibles

Toutes les failles susmentionnées peuvent être exploitées sous certaines circonstances pour exécuter un code à distance sur les systèmes concernés. Par conséquent, les objectifs de sécurité (confidentialité, intégrité et disponibilité) ne peuvent plus être garantis. Certaines des failles mentionnées sont utilisées entre autres par les variantes de malware connues « WannaCry » [5] et « NotPetya » [6].

Aucun cas d'accès abusif obtenu via les failles mentionnées n'a été signalé pour les appareils Miele.

Mesures préventives

Nous souhaitons ajouter que les appareils Miele mentionnés ci-dessus ne sont **pas** prévus pour être connectés directement à Internet.

Comme mesure de sécurité, des mises à jour de sécurité seront installées gratuitement par un technicien Miele dans le cadre de la maintenance annuelle.

Nous vous conseillons **par ailleurs** pour continuer à réduire les risques de procéder de manière standard aux mesures suivantes et d'exploiter votre appareil exclusivement sous cette forme :

- N'autorisez en aucun cas un accès à distance vers l'appareil par Internet (par exemple par redirection de port). Si votre appareil est accessible via Internet, désactivez immédiatement cette connexion.
- Exploitez les appareils exclusivement dans un segment réseau distinct et séparé physiquement. Réservez exclusivement ce réseau aux systèmes nécessaires à la traçabilité des résultats de traitement (par ex. : PC et imprimante).
- Limitez l'accès au stérilisateur et aux systèmes autorisés uniquement au personnel prévu pour les utiliser.
- Protégez les systèmes autorisés par un mot de passe pertinent.
- Modifiez régulièrement les mots de passe enregistrés sur les appareils (voir le manuel de programmation).

Concernant le reste de la procédure, veuillez vous adresser à votre commercial Miele compétent.

Veuillez-vous assurer que cet avertissement soit consigné dans le mode d'emploi de votre produit.

Veuillez transmettre ces informations à l'administrateur du réseau et à tout le personnel concerné.

Interlocuteur

Votre interlocuteur chez Miele est :

Jean-Louis PUYSSEGUR – Medical Product Officer Miele France
9 avenue Albert Einstein – 93150 LE BLANC MESNIL
Tél : +33 1 49 39 44 64 / +33 6 89 71 43 04
jean-louis.puyssegur@miele.com

Nous restons disponibles pour toute question. En vous remerciant de vote coopération,

Veuillez noter que nous vous informerons activement à l'avenir sur **https://psirt.miele.com** sur les sujets relatifs à la cybersécurité dans l'environnement de nos appareils. Nous fournirons également des rapports sur les failles actuelles.

Cordialement,

Sources :

[1] Microsoft article KB KB4019264 :
https://support.microsoft.com/fr-fr/help/4019264/windows-7-update-kb4019264
[2] Microsoft Security Bulletin MS08-067 :
https://technet.microsoft.com/fr-fr/library/security/ms08-067.aspx
[3] Microsoft Security Bulletin MS15-034 :
https://docs.microsoft.com/fr-fr/security-updates/securitybulletins/2015/ms15-034
[4] Microsoft Security Bulletin MS14-066 :
https://docs.microsoft.com/fr-fr/security-updates/securitybulletins/2014/ms14-066
[5] Informations sur le logiciel malveillant « WannaCry »
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
https://fr.wikipedia.org/wiki/WannaCry_ransomware_attack
[6] Informations sur le logiciel malveillant « NotPetya »
https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine