Anschreiben bei CX1020 Steuerung

Wichtiger Hinweis für die Miele Sterilisationsgeräte PS5XXX

Sehr geehrte….(ZSVA-Leiter bzw. Laborleiter bzw. Praxisinhaber, Empfänger einsetzen),

nach unseren Unterlagen sind in Ihrem Hause Sterilisatoren des Typs PS5 XXXX von Miele im Einsatz. Diese Geräte sind mit einer Netzwerkschnittstelle ausgestattet, mit denen sie sich zur Chargendokumentation an ein lokales Netzwerk anschließen lassen.

Mit diesen Schreiben möchten wir Sie darüber informieren, dass wir im Rahmen von unseren regelmäßigen Sicherheitsüberprüfungen Kenntnisse über **Schwachstellen des im Gerät verwendeten Microsoft Betriebssystem** erlangt haben.

Es handelt sich dabei um folgende Schwachstellen:

Betroffene Applikation	Information über Schwachstelle	CVE
Microsoft Windows SMB-Dienst	MS08-067 [1]	CVE-2008-4250
Microsoft Windows SMB-Protokoll	MS09-001 [2]	CVE-2008-4834 CVE-2008-4835 CVE-2008-4114
Microsoft Windows SMB-Server	MS17-010 [3]	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148
Microsoft Windows Remotedesktop-Dienst	MS12-020 [4]	CVE-2012-0002 CVE-2012-0152

Mögliche Risiken

Alle genannten Schwachstellen können unter Umständen für eine Remotecodeausführung auf den betroffenen Systemen ausgenutzt werden. Dadurch können die Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) nicht mehr garantiert werden. Einige der benannten Schwachstellen werden unter anderem durch die bekannten Malware Varianten „WannaCry“ [5] und „NotPetya“ [6] ausgenutzt.

Aktuell ist uns kein Fall bekannt, bei dem über die genannten Schwachstellen bei den genannten Miele-Geräten missbräuchlicher Zugang erlangt wurde.

Vorbeugende Maßnahmen

Wir weisen darauf hin, dass die oben bezeichneten Miele-Geräte **nicht** dafür vorgesehen sind, direkt mit dem Internet verbunden zu werden.

Als eine sichernde Maßnahme werden Sicherheitsupdates durch einen Miele-Servicetechniker im Rahmen der jährlichen Wartung kostenfrei installiert.

Wir empfehlen Ihnen **zusätzlich** zur weiteren Minimierung von Risiken, die nachfolgenden Maßnahmen standardmäßig umzusetzen und das Gerät ausschließlich in dieser Form zu betreiben:

- Ermöglichen Sie keinesfalls den Zugriff auf das Gerät über das Internet (z. B. durch Portweiterleitung). Falls Ihr Gerät heute dennoch über das Internet erreichbar ist, unterbinden Sie diesen Zugriff sofort.

- Betreiben Sie die Geräte nur in einem separaten und physisch Netzwerksegment. In diesem Netzwerk dürfen nur die für die Dokumentation der Aufbereitungsergebnisse benötigten Systeme (z.B. PC und Drucker) betrieben werden.

- Beschränken Sie den Zugang zu dem Gerät und den zugriffsberechtigten Systemen auf den notwendigen Personenkreis.

- Sichern Sie die zugriffsberechtigten Systeme über starke Passwörter.

- Ändern Sie regelmäßig bestehende Passwörter auf den Geräten (siehe Programmierhandbuch).

Für das weitere Vorgehen wenden Sie sich bitte an Ihren zuständigen Miele Vertriebspartner.

Sorgen Sie bitte dafür, dass dieser Kundenwarnhinweis in der Gebrauchsanweisung Ihres Systems hinterlegt wird. Bitte geben Sie diese Information an den Netzwerkadministrator weiter und auch an alle Mitarbeiterinnen und Mitarbeiter, die es betrifft.

Ihr Ansprechpartner bei Miele ist:

…(MPO der VG)
(Anschrift, Rufnummer, FAX-Nr., E-Mail)

Wir stehen Ihnen für Rückfragen gerne zur Verfügung – und bedanken uns für Ihre Kooperation.

Bitte beachten Sie, dass wir Sie in Zukunft auf https://psirt.miele.com aktiv zu Cybersecurity Themen im Umfeld unserer Geräte informieren werden. Dazu zählen auch Meldungen zu aktuellen Schwachstellen.

Mit freundlichen Grüßen

…

Quellen:

[1] Microsoft Security Bulletin MS08-067:
https://technet.microsoft.com/de-de/library/security/ms08-067.aspx
[2] Microsoft Security Bulletin MS09-001:
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-001
[3] Microsoft Security Bulletin MS17-010:
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
[4] Microsoft Security Bulletin MS12-020:
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020
[5] Informationen zur Schadsoftware “WannaCry”
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[6] Informationen zur Schadsoftware „NotPetya“
https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine