

Miele & Cie. KG, Postfach, 33325 Gütersloh

Address of customer

Your reference/message from

Our reference

Phone 05241 89-

Fax 05241 89-

Date

BMP/QM

Thursday, 5<sup>th</sup> of June 2018

## Letter relating to CX2020 controls

### Miele guideline on cybersecurity on PS5XXX sterilisers

Dear ....(CSSD or laboratory manager, surgery owner, ...)

According to documents held by us, PS5xxx sterilisers from Miele are deployed in your hospital. These machines feature a network interface for connection to a local network for documentation purposes.

The purpose of this correspondence is to inform you that **vulnerabilities in the Microsoft operating system** used on this model have been found in the course of regular software checks.

These are as follows:

Application affected	Information on vulnerability	CVE
Microsoft Windows SMBv1 protocol	The Microsoft service SMBv1 (Port 445) contains various flaws which could result in the disclosure of information, a system crash or the execution of remote code when executed. [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

Application affected	Information on vulnerability	CVE
		CVE-2017-0277 CVE-2017-0278 CVE-2017-0279
Microsoft Windows SMB server	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 RDP service (Port 3389)	MS14-066 [4]	CVE-2014-6321

### Possible consequences

All the above-mentioned vulnerabilities could, given the right circumstances, be used to execute remote code on the affected systems. This may jeopardise your attempts to achieve your safeguarding objectives (confidentiality, integrity and availability). Several of the vulnerabilities mentioned above are used, among others, by known malware versions such as WannaCry [5] and NotPetya [6].

We are not currently aware of any case in which the above-mentioned vulnerabilities on Miele Machines have resulted in improper access.

### Preventative measures

The Miele machines listed above are **not** designed for direct connection to the Internet.

**A Miele service technician will install security updates during the yearly on-site maintenance. The installation will be free of charge.**

**Additionally**, we always recommend routinely implementing the following measures and only using the machine in the specified manner:

- Do not enable access to the machine via the Internet (e.g. through port forwarding). If your machine is nevertheless linked to the Internet, sever any Internet connections immediately.

- Only operate these machines in a physically separated section of the network. In this network, only the systems required for the documentation of reprocessing results (e.g. PC and printer) should be operated.
- Limit access to any affected machine and access-authorized systems exclusively to persons requiring access in the course of their work.
- Secure access-authorized systems using strong passwords.
- Alter existing passwords on machines at regular intervals (cf. programming manual).

Please contact your Miele sales representative to discuss further steps.

Please ensure that this guideline on cyber security is properly filed. Please also forward this information to network administrators and all members of staff affected.

Your contact at Miele is:

...(MPO of subsidiary)  
(address, contact no, fax no. or email)

We apologise for this inconvenience, are available to answer any questions you may have, and thank you very much in advance for your cooperation.

Please note that we will in future be actively posting on cyber security issues relating to our machines on <https://psirt.miele.com>. These will also include reports on current vulnerabilities.

Kind regards,

Miele Werk Bürmoos GmbH



Tel.: +43 (0) 6274 6344 89396  
Mobile: +43 (0) 664 664 8542485  
Fax: +43 (0) 6274 6344 89120

**Sources:**

[1] Microsoft KB-Artikel KB4019264:

<https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264>

[2] Microsoft Security Bulletin MS08-067:

<https://technet.microsoft.com/de-de/library/security/ms08-067.aspx>

[3] Microsoft Security Bulletin MS15-034:

<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034>

[4] Microsoft Security Bulletin MS14-066:

<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-066>

[5] Information on WannaCry malware

[https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

[6] Information on NotPetya malware

[https://en.wikipedia.org/wiki/2017\\_cyberattacks\\_on\\_Ukraine](https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine)

# Response form

Client

**Important safety-relevant information / Urgent client information for corrective action in the field - IT security vulnerability**

Dear Sir or Madam,

We herewith confirm receipt of your safety-relevant information/client information on corrective action in the field dated Tuesday, 5<sup>th</sup> of June 2018

. We have read and understood the recommendations of the medical device manufacturer.

The machines are connected to a network:

Yes

No

Name/Function: \_\_\_\_\_

Hospital/Surgery/Laboratory: \_\_\_\_\_

Street/No: \_\_\_\_\_

Type/Serial-No: \_\_\_\_\_

Postal code, town: \_\_\_\_\_

Place, date \_\_\_\_\_

Signature \_\_\_\_\_

