Customer Advisory Notice
CAN 003-2017

To: Director of the Radiology Department
Director of the Nuclear Medicine / PET lmaging Department
Risk Management Officer
Users of Siemens SPECT, SPECT.CT, PET, PET.CT Systems and Workplaces

Re: Microsoft Software Vulnerabilities

Dear Valued Siemens Healthineers Customer,

We have become aware of Microsoft software vulnerabilities, which may impact your system. Recently, Microsoft announced a series of vulnerabilities in their Server Message Block version 1.x (SMBv1) implementation.

What are the potential risks?

Based on our assessment of the malware exploitations and the potential impact to our products, we will be providing patches as one option to resolve the SMBv1 vulnerabilities . These vulnerabilities could allow remote code execution on your Molecular lmaging medical device. One exploit of these vulnerabilities has already surfaced and is code-named "WannaCry." This exploit could allow ransomware to be installed on infected computer systems.

We currently have no reports of adverse events related to this issue on any Molecular lmaging systems.

Siemens Medical Solutions USA, Ine.
2501 N. Barrington Rd.
Hoffman Estates, IL 60192, USA

What are the potential mitigations?

The table lists the minimum version of software required to receive a patch:

Product	Minimum Version Required to Receive Patch
SPECT E.CAM	VA46A
SPECT Symbia E	VA60A
SPECT Symbia S	VA60A
SPECT Svmbia T/T2/T6/T16	VA60A
SPECT Symbia lntevo T/T2/T6/T16	VB10A
SPECT Symbia lntevo Bold	VB20A
SPECT Symbia Evo	VB10A
SPECT Symbia Evo Excel	VB10A
SPECT Symbia.net	VA10C
SPECT Ml Workplaces (V, P, C)	VA60A
PET Bioqraph HiRez 6/16	6.6.x (VF?Ox)
PET Biograph TruePoint 6/16/40/64	6.0.6 (VF16A), 6.5.4 (VF64A)
PET Bioqraph mCT and mCT Flow	VG50x
PET Horizon	VJ10x
PET Advanced Workflow (Wizards)	Based on scanner version(s) above

Devices with software version VA70 are not eligible to receive a patch. lnstead, these devices should upgrade to version VB10. Once upgraded, the patch can be applied.

The software version of your system can be found from the main menu of the software. Simply choose **HELP I ABOUT "Your Product"** from the menu system, where "Your Product" is the name of the product in question. If you have any difficulties determining your software version, please contact Siemens service at the contact numbers provided within this letter.

If your system meets the minimum software version indicated in this letter, there are two ways for you to obtain the software patch:

1. If Siemens provides your service and you're connected to Siemens Remote Services (SRS), then the patch will be pushed to you automatically via Remote Update Handling (RUH).
2. If you are not connected to SRS, then you will be contacted by Siemens in order to install the patch on your system.

In the event that your system does not meet the minimum software version indicated in this letter, there are other mitigations available to you:

1. A hardware firewall can be employed to block ports 139/tcp, 445/tcp or 3389/tcp, or
2. Your system can be disconnected from your local network

Due to the nature of these Microsoft software vulnerabilities, if your system is not at the minimum software version required to receive a patch, Siemens Healthineers strongly recommends that you select one of the above options to prevent your Molecular Imaging system from becoming infected with malware.

Please ensure that this customer advisory notice is placed in your system's Operator's Manual and this information is disseminated to all operators of the system. If this equipment is no longer in your possession, we kindly ask that you forward this letter to the new owner of the equipment, and inform Siemens about the change in ownership.

Adverse events or quality problems experienced with the use of your device should be reported to Siemens through the contact information provided below.

If you have any questions regarding this advisory notice, please contact your local Siemens representative at the contact numbers provided below.

- America: 1-800-888-7436
- Europe, Middle East, and Africa: +49 9131 940 4000
- Asia and Australia: +86 (21) 3811 2121

Additional Resources:

[1] Microsoft Security Bulletin MS17-010:
https://technet.microsoft.com/en-us/library/security/ms17-01O. aspx
[2] For more information on security advisories associated with these vulnerabilities, please visit our Siemens ProductCERT website
http://www.siemens.com/cert/en/cert-security-advisories .htm

Sincerely,

……..
……
……
……

Siemens Medica! Solutions USA, Ine.
2501 N. Barrington Rd.
Hoffman Estates, IL 60192, USA