ID number: **TH008/17/S**

Customer Information Letter

Re.: Customer Information Letter regarding Microsoft Windows vulnerability (MS17-010)
- **RTT 1.6**
- **RTT 4.1 / RTT 4.1 Assist**
- **Lantis System (Pre 2003)**

Attention: Radiation Oncology Department

Dear Customer,

This letter is intended to inform you about a vulnerability in Windows operating systems from Microsoft.

What is the issue?

Radiation Oncology products from Siemens Healthineers are potentially affected by the vulnerability described in the Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/library/security/MS17-010).

Although not explicitly mentioned in MS17-010, Microsoft Windows XP® and earlier versions, including Windows 2000, are affected.

What could be the ramifications?

All systems infected by the so called “WannaCry” malware may experience the following:

- A total system shut down
- A loss of patient data

This may have major impact on the documentation and quality of the entire patient treatment.

Siemens Healthcare GmbH
Henkestraße 127
D-91052 Erlangen
Germany

Print number: **TH11-400.691.09.01.02**

What will Siemens do to address this issue?

Microsoft has released a patch to address the Windows vulnerability for a selection of Windows operating system versions (KB4012598). The following Siemens products

- RTT 1.6
- RTT 4.1 / RTT 4.1 Assist
- Lantis System (Pre 2003)

do not meet the Windows operating system requirements for this patch to be installed.

The exploitability of this vulnerability depends on the actual configuration and deployment environment of each product. Therefore, Siemens Healthineers recommend the following:

- For vulnerable products that are listening on network ports 139/tcp, 445/tcp or 3389/tcp, their exploitation exposure depends on the security measures within the network. In order to protect a vulnerable product from exploitation it should be isolated from any potentially infected system within its respective network segment (e.g. product deployed in a network segment separated by firewall control blocking access to network ports 139/tcp, 445/tcp and 3389/tcp).
- If patient safety and treatment is not at risk (in particular when device is in stand-by-mode), always disconnect the product from the network.
- In any case, ensure to have appropriate backups and system restoration protocols in place.

Please follow the recommendations and include this Customer Information Letter into your user documentation, where it should remain.

We regret any inconvenience that this may cause, and we thank you in advance for your understanding.

Sincerely,

signed Dr. Gabriel Haras
Head of AT RO

signed René Lennert
Head of AT RO Quality Management

This document is valid without original signature.

Siemens Healthcare GmbH
Henkestraße 127
D-91052 Erlangen
Germany

Print number: **TH11-400.691.09.01.02**