ID number: **TH003/19/S**

Field Safety Notice

Re.: Field Safety Notice- Applicable to your LANTIS™ Oncology Information System Server

CC: Chairman of Medical Board & Heads of Departments

Attention: Radiation Oncology Department

Dear Customer,

This letter is intended to inform you about a potential safety risk related to patient treatment when using LANTIS™ Oncology Information System Server software.

What is the issue and when does it occur?

Select Radiation Oncology products from Siemens Healthineers are potentially affected by the Microsoft Windows Remote Desktop Protocol (RDP) vulnerability, see

Customer guidance for CVE-2019-0708 (Remote Desktop Services Remote Code Execution Vulnerability), May 14, 2019 at: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708.

The exploitability of the vulnerabilities depends on the actual configuration and deployment environment of each product.

According to Microsoft this vulnerability, once exploited, allows remote code execution on the infected system.

A LANTIS system server infected by a potential malware exploiting this vulnerability, may be affected in different ways, including but not limited to:

- A system crash or unintended reboot
- A total system down
- 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: **TH06-021.691.07.01.02**

Microsoft has released a patch for a selection of Windows operating system versions. If your LANTIS system server is running the Microsoft Windows Server 2003 SP2 x86 operating system version, a patch for your system can be found at:

Customer guidance for CVE-2019-0708 (Remote Desktop Services Remote Code Execution Vulnerability), May 14, 2019 at: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708.

However, since the LANTIS Oncology Information System had already reached end of support on March 31, 2016 we did not test and validate the patch, thus we cannot assume any liability whatsoever for its compatibility and safe operation of the device. Installing the patch on the device would be at your own risk.

We strongly recommend the following:

- Disable Remote Desktop Protocol (RDP) or close port 3389/tcp

In addition, Siemens Healthineers recommends:

- Ensure you have appropriate backups and system restoration procedures.
- For additional information contact your local Siemens Healthineers Customer Service Engineer, portal or our Regional Support Center.

Additional information

- Please note that Microsoft Windows Server 2003 is the latest operating system released for use with LANTIS system server. More details can be found in TH023/14/S.
- Furthermore we would like to remind you that the LANTIS Oncology Information System reached end of support on March 31, 2016. We therefore strongly recommend to replace the LANTIS Oncology Information System by a new oncology information system.

Please include this Field Safety Notice in your Siemens LANTIS System Owner Manual, where it should remain.

The relevant National Competent Authority will be informed of this Field Safety Notice.

Siemens Healthcare GmbH
Henkestraße 127
D-91052 Erlangen
Germany

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

Sincerely,

signed Dr. Gabriel Haras
Head of Business Segment RO

signed René Lennert
Head of RO Segment Quality Management

This document is valid without original signature.

Siemens Healthcare GmbH
Henkestraße 127
D-91052 Erlangen
Germany