SIEMENS
Healthineers

Siemens Healthcare GmbH, HC DI SY, Henkestr. 127, 91052 Erlangen

| | |
|---|---|
| Name | Vincent Schets |
| Department | HC SV DS PLM PACS |
| Telephone | +49 (9131) 84-8169 |
| Our reference | SY029-17-S |
| Date | May 29, 2017 |

## CUSTOMER ADVISORY NOTICE

To all users of products described under PRODUCT SPECIFIC INFORMATION

**Customer Information on WannaCry Malware for Siemens Healthineers Syngo and Digital Health Services Products**

Dear customer,

Siemens Healthineers recognizes that your organization may be facing impacts from the recent major cyber-attack known as “WannaCry”.

## What is the issue and when does it occur?

Select Siemens Healthineers products may be affected by the Microsoft vulnerability being exploited by the WannaCry ransomware. The exploitability of any such vulnerability depends on the actual configuration and deployment environment of each product. According to Microsoft this ransomware spreads either by attachments/links in phishing emails or on malicious websites (“system zero infection”) or via an infected system that exploits a vulnerability in a Windows component used in the context of open file shares of other systems reachable on the same network.

Certain details may be found on the following Microsoft page:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

We would like to point out that neither the use of an email client nor browsing the internet is part of the intended use of most of the products covered by this letter.

**Siemens Healthcare GmbH**
Management: Bernhard Montag, Vorsitzender;
Thomas Rathmann, Michael Reitermann

Henkestr. 127
91052 Erlangen
Deutschland

Tel.: +49 (9131) 84 0
Fax: +49 (9131) 84 0
www.siemens.com/healthcare

Chairman of the Supervisory Board: Michael Sen;
Registered office: München, Germany; Commercial Registry: Munich, HRB 213821
WEEE-Reg.-Nr. DE 64872105

SCF 02/2015 V13.06

Page 1 of 3

## What steps can the user take to avoid the issue?

Products that are not listening on network ports 139/tcp, 445/tcp and 3389/tcp should not expose the vulnerability provided the product is used according to the intended use and standard configuration.

Siemens Healthineers provides a list of products (see next section) that can be patched by customers according to the Microsoft Security Bulletin MS17-010 [https://technet.microsoft.com/en-us/library/security/ms17-010.aspx] and recommends patches be applied immediately. Additionally, Siemens Healthineers issues Siemens Security Advisories for select products that require specific remediation information.

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 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 the above cannot be implemented we recommend the following:

- If patient safety and treatment is not at risk, disconnect the uninfected product from the network and use in standalone mode.
- Reconnect the product only after the provided patch or remediation is installed on the system.

In addition, Siemens Healthineers recommend:

- Ensure you have appropriate backups and system restoration procedures.
- Ensure you apply most recent security updates.
- For specific patch and remediation guidance information contact your local Siemens Healthineers Customer Service Engineer, portal or our Regional Support Center.

## PRODUCT SPECIFIC INFORMATION

The Microsoft security patches can be installed in conjunction with the following Siemens Healthineers products and products distributed by Siemens Healthineers:

- *syngo*.via®: All versions
- *syngo*.via Frontier: All versions
- *syngo*.via ProtoNeo: All versions
- *syngo*.WebViewer: All versions
- *syngo*.Dynamics: All versions
- *syngo*.plaza®: All versions
- *syngo*® Imaging: All Versions on OPM server and syngo Studio Advanced
- *syngo*® Workflow MLR: All versions
- *syngo*® Workflow SLR: All versions
- teamplay®: All versions
- syngo Imaging XS: All versions on Servers and Reporting clients
- MagicLink A: all versions
- SIENET MagicWeb Server: All versions up to VA50B_0207
- MagicView 1000W: Version VF50A and newer
- ResolutionMD: All versions

In case additional measures are needed, additional product specific information will be sent out.

For further information please visit our ProductCERT Security Advisories site.
http://www.siemens.com/cert/

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

Sincerely Yours

Dr. Frank Engel-Murke
Head of DS PACS Define

Oliver Klinkow
VP Marketing & Sales