SSB-412479: Customer Information on WannaCry Malware for Siemens Healthineers Imaging and Diagnostics Products

Publication Date 2017-05-16
Last Update 2017-06-14
Current Version V1.5

DESCRIPTION

Siemens Healthineers recognizes that some of its customers may be facing impacts from the recent major cyber-attack known as “WannaCry”.

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 product types covered by this Siemens Security Bulletin.

RECOMMENDATIONS

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 [1] 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. Siemens Healthineers is able to patch systems capable of Remote Update Handling (RUH) much faster by remote software distribution compared to onsite visits. Therefore customers of RUH capable equipment are recommended to clarify the situation concerning patch availability and remaining risk in the local customer network with the Siemens Customer Care Center first and then to re-connect their systems in order to receive patches as fast as possible via Remote Update Handling. This ensures smooth and fast receipt of updates and therefore supports re-establishment of system operations.

In addition, Siemens Healthineers recommend:

- Ensure you have appropriate backups and system restoration procedures.
- 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 patches can be installed in conjunction with the following Siemens Healthineers products:

- *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 servers and syngo Studio Advanced clients
- *syngo*® Imaging XS: All versions on servers and Reporting Clients
- *syngo*® Workflow MLR: All versions
- *syngo*® Workflow SLR: All versions
- teamplay®: All versions
- Atellica Process Manager: All versions
- *syngo* Lab Inventory Manager: All versions
- PRISCA: All versions
- CentraLink: All versions
- Xprecia Stride™ Data Management System (DMS): All versions
- RAPIDComm® Data Management System: All versions
- POCcelorator™: All versions
- UniPOC™: All versions
- RapidLink™: All versions
- SIENET MagicWeb Server: All versions up to VA50B_0207
- SIENET MagicView 1000W: Version VF50A and newer

Siemens Healthineers published the following Siemens Security Advisories:

- SSA-832636: SMBv1 Vulnerabilities in Magnetic Resonance Products from Siemens Healthineers [2]
- SSA-354910: SMBv1 Vulnerabilities in Multi-Modality Workplace (MMWP) Products from Siemens Healthineers [3]
- SSA-286693: SMBv1 Vulnerabilities in Laboratory Diagnostics Products from Siemens Healthineers [4]
- SSA-408571: SMBv1 Vulnerabilities in Computed Tomography Products from Siemens Healthineers [5]
- SSA-492736: SMBv1 Vulnerabilities in Radiography, Mobile X-ray and Mammography Products from Siemens Healthineers [6]

- SSA-966341: SMBv1 Vulnerabilities in Molecular Diagnostics Products from Siemens Healthineers [7]
- SSA-023589: SMBv1 Vulnerabilities in Advanced Therapy Products from Siemens Healthineers [8]
- SSA-740012: SMBv1 Vulnerabilities in Biograph mMR from Siemens Healthineers [9]
- SSA-774661: SMBv1 Vulnerabilities in Radiation Oncology Products from Siemens Healthineers [10]
- SSA-709509: SMBv1 Vulnerabilities in Point-of-Care Products from Siemens Healthineers [11]
- SSA-701903: SMBv1 Vulnerabilities in Ultrasound Products from Siemens Healthineers [12]
- SSA-161640: SMBv1 Vulnerabilities in Molecular Imaging Products from Siemens Healthineers [13]

If you cannot find your specific product or have further questions, please refer to your local Siemens customer support.

ADDITIONAL RESOURCES

[1] Microsoft Security Bulletin MS17-010: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[2] SSA-832636: SMBv1 Vulnerabilities in Magnetic Resonance Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-832636.pdf

[3] SSA-354910: SMBv1 Vulnerabilities in Multi-Modality Workplace (MMWP) Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-354910.pdf

[4] SSA-286693: SMBv1 Vulnerabilities in Laboratory Diagnostics Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-286693.pdf

[5] SSA-408571: SMBv1 Vulnerabilities in Computed Tomography Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-408571.pdf

[6] SSA-492736: SMBv1 Vulnerabilities in Radiography, Mobile X-ray and Mammography Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-492736.pdf

[7] SSA-966341: SMBv1 Vulnerabilities in Molecular Diagnostics Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-966341.pdf

[8] SSA-023589: SMBv1 Vulnerabilities in Advanced Therapy Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

[9] SSA-740012: SMBv1 Vulnerabilities in Biograph mMR from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-740012.pdf

[10] SSA-774661: SMBv1 Vulnerabilities in Radiation Oncology Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-774661.pdf

[11] SSA-709509: SMBv1 Vulnerabilities in Point-of-Care Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-709509.pdf
[12] SSA-701903: SMBv1 Vulnerabilities in Ultrasound Products from Siemens Healthineers https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-701903.pdf
[13] SSA-161640: SMBv1 Vulnerabilities in Molecular Imaging Products from Siemens Healthineers: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-161640.pdf

HISTORY DATA

V1.0 (2017-05-16):	Publication Date
V1.1 (2017-05-17):	Extended recommendations
V1.2 (2017-05-19):	Extended product-specific information
V1.3 (2017-05-22):	Extended product-specific information
V1.4 (2017-06-01):	Extended product-specific information
V1.5 (2017-06-14):	Extended product-specific information and added information on Remote Update Handling (RUH)

DISCLAIMER