SSA-774661: SMBv1 Vulnerabilities in Radiation Oncology Products from Siemens Healthineers

Publication Date 2017-05-19
Last Update 2017-09-01
Current Version V1.2
CVSS v3.0 Base Score 9.8

SUMMARY

Select Radiation Oncology products from Siemens Healthineers are affected by the Microsoft Windows SMBv1 vulnerabilities. The exploitability of the vulnerabilities depends on the actual configuration and deployment environment of each product.

Siemens Healthineers has developed solutions for the supported affected products which are available via customer support.

AFFECTED PRODUCTS

- RTT: All versions
- Coherence Therapist / Primeview 3i: All versions without TH007/17/S
- Coherence Oncologist: All versions
- Coherence Dosimetrist: All versions
- Coherence Physicist: All versions
- Syngo RT Therapist 4.1: All versions
- Syngo RT Therapist 4.2: All versions without TH007/17/S
- Syngo RT Therapist 4.3: All versions without TH007/17S
- Syngo RT Oncologist: All versions without TH007/17/S
- Syngo RT Dosimetrist: All versions without TH007/17/S
- ModuLeaf: All versions
- Simview 3000/NT: All versions
- Beamview NT: All versions
- Lantis Commander 6.1: All versions without TH066/17/S
- Lantis Commander 8.3: All versions without TH066/17/S
- Mosaiq (Elekta product): All versions

DESCRIPTION

Siemens Healthineers radiation oncology products are used in hospital environments for patient treatments.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-0143)

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Vulnerability 2 (CVE-2017-0144)

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Vulnerability 3 (CVE-2017-0145)

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Vulnerability 4 (CVE-2017-0146)

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

Vulnerability 5 (CVE-2017-0147)

An authenticated remote attacker could potentially disclose information from the server by sending specially crafted packets to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Vulnerability 6 (CVE-2017-0148)

An unauthenticated remote attacker could execute arbitrary code via specially crafted requests sent to the SMBv1 server of affected Microsoft Windows systems.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

SOLUTION

Siemens Healthineers offers security updates for the following software versions via its customer support:

- Coherence Therapist / Primeview 3i: software update TH007/17/S
- Syngo RT Therapist 4.2: software update TH007/17/S
- Syngo RT Therapist 4.3: software update TH007/17S
- Syngo RT Oncologist: software update TH007/17/S
- Syngo RT Dosimetrist: software update TH007/17/S
- Lantis Commander 6.1 (based on Windows Server 2003 SP2): software update TH066/17/S
- Lantis Commander 8.3 (based on Windows Server 2003 SP2): software update TH066/17/S

For questions regarding the update procedure, please contact customer service.

Until patches can be applied by the customer support, and for end-of-support products, we recommend that affected products that are listening on network ports 139/tcp, 445/tcp or 3389/tcp be isolated from any infected system within the respective network segment (e.g. by firewall blocking access to above network ports.)

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 recommends:

- 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.

ADDITIONAL RESOURCES

[1] Customer Information on WannaCry Malware for Siemens Healthineers Imaging and Diagnostics Products is available here:
https://www.siemens.com/cert/pool/cert/siemens_security_bulletin_ssb-412479.pdf

[2] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-05-19): Publication Date
V1.1 (2017-06-14): Added information on Remote Update Handling (RUH)
V1.2 (2017-09-01): Updated solution information

DISCLAIMER