SSA-023589: SMBv1 Vulnerabilities in Advanced Therapy Products from Siemens Healthineers

Publication Date 2017-05-19
Last Update 2017-06-14
Current Version V1.2
CVSS v3.0 Base Score 9.8

SUMMARY

Select Advanced Therapy 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 is working on updates for the affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS

- AXIOM Artis: All versions without AX038/17/S
- Artis one, Q and pheno: All versions without AX039/17/S
- Artis zee:
  - All versions (except VD11B, VD11C) without AX038/17/S
  - Versions VD11B, VD11C without AX039/17/S
- Sensis: AQU: All versions without AX046/17/S
- Sensis PPWS: All versions without AX046/17/S
- Sensis HES: All versions without AX046/17/S
- Sensis SIS: All versions without AX046/17/S
- Sensis VM Server: All versions without AX046/17/S
- Leonardo/X-Workplace:
  - All versions (except VD10E, VD11B, VD20B) without AX041/17/S
  - Versions VD10E, VD11B, VD20B without AX042/17/S
- Arcadis family: All versions without AX043/17/S

DESCRIPTION

Siemens Healthineers Advanced Therapies (AT) products are used in interventional laboratories and (hybrid) ORs for diagnostic and therapeutic procedures.

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 provides security updates that will be automatically available for customers with remote support for the following software versions of the affected devices:

- AXIOM Artis update to AX038/17/S for versions: VB23N, VB23P, VB35D, VB35E
- Artis one update to AX039/17/S for version VA10D
- Artis Q update to AX039/17/S for versions: VD10E, VD11B, VD11C
- Artis pheno update to AX039/17/S for versions: VE10A, VE10B
- Artis zee update to AX038/17/S for versions: VC14H, VC14J, VC21B, VC21C
- Artis zee update to AX039/17/S for versions: VD11B, VD11C
- Leonardo/X-Workplace update to AX041/17/S for versions: VB13F, VB13N, VB14C, VB15D, VB20D, VB21C, VB21N, VC10D, VC10N
- Leonardo/X-Workplace update to AX041/17/S for versions: VD10E, VD11B, VD20B

Siemens Healthineers provides security updates for local installation for the following products:

- Arcadis Varic update to AX043/17/S for version VC10A
- Arcadis Orbic update to AX043/17/S for version VC10A

- Arcadis Avantic: update to AX043/17/S for version VC10A
- Sensis: AQU update to AX046/17/S for versions: VC03E, VC03F, VC03G, VC11D, VC12B, VC12C, VC12L, VD10B
- Sensis PPWS update to AX046/17/S for versions: VC03E, VC03F, VC03G, VC11D, VC12B, VC12C, VC12L, VD10B
- Sensis HES update to AX046/17/S for versions: VC03E, VC03F, VC03G, VC11D, VC12B, VC12C, VC12L, VD10B
- Sensis SIS update to AX046/17/S for versions: VC03E, VC03F, VC03G, VC11D, VC12B, VC12C, VC12L, VD10B
- Sensis VM Server update to AX046/17/S for versions: VC12L, VD10B

If no remote support is available or 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, Siemens Healthineers recommends to isolate affected products that are listening on network ports 139/tcp, 445/tcp or 3389/tcp from any infected system within its 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 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.

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 (2017-06-09): Added update information
V1.2 (2017-06-14): Added information on Remote Update Handling (RUH)

DISCLAIMER