SSA-408571: SMBv1 Vulnerabilities in Computed Tomography Products from Siemens Healthineers

Publication Date 2017-05-17
Last Update 2017-06-14
Current Version V1.2
CVSS v3.0 Base Score 9.8

SUMMARY

Computed Tomography 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 provides updates for the supported affected products and recommends specific countermeasures until patches are available.

AFFECTED PRODUCTS

- SOMATOM® Drive and Confidence: All versions without VA62A_FP10 installed
- SOMATOM® Force, Definition Edge, Definition Flash, Definition/ Definition AS family: All versions without Som7_FP10 installed
- Other SOMATOM® CT: All versions without ServPack41 or ServPack42 installed

DESCRIPTION

Siemens Healthineers Computed Tomography products are used in network-connected hospital environments for imaging.

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 for the following software versions of the affected devices:

- SOMATOM® Drive and Confidence: VA62A_FP10 for VA62
- SOMATOM® Force, Definition Edge, Definition Flash, Definition/ Definition AS family: Som7_FP10 for VA44A, VA48A, and VA50A
- Other SOMATOM® CT: ServPack41 for VC20B, VC28A, VC30B, VC40A
- Other SOMATOM® CT: ServPack42 for VB20, VB26, VB27, VB28, VB36, VB42

The update will be automatically available for customers with remote support. If no remote support is available or for questions regarding the update procedure, please contacts customer service.

The correct installation can be verified in the main syngo under “Options -> Versions”, ensuring the respective security update is listed under Siemens software packages.

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 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 (2017-05-17): Publication Date
V1.1 (2017-05-29): Added update information
V1.2 (2017-06-14): Added information on Remote Update Handling (RUH)

DISCLAIMER