SSA-701903: SMBv1 Vulnerabilities in Ultrasound Products from Siemens Healthineers

Publication Date: 2017-05-22
Last Update: 2018-02-22
Current Version: V1.3
CVSS v3.0 Base Score: 9.8

SUMMARY

Select Ultrasound 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 provides updates for the affected products, and recommends specific countermeasures until patches can be applied.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
ACUSON P300™ ultrasound system: Version V13.02 without US025/17/S	Install US025/17/S Please contact customer service.
ACUSON P300™ ultrasound system: Version V13.03 and V13.21 without US012/17/S	Install US012/17/S Please contact customer service.
ACUSON P300™ ultrasound system: Version V13.20 without US026/17/S	Install US026/17/S Please contact customer service.
ACUSON P500™ ultrasound system VA10: Version VA10 without US015/17/S	Install US015/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “Config -> Select Device -> Verify”
ACUSON P500™ ultrasound system VB10: Version VB10 without US016/17/S	Install US016/17/S 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 contact customer service. The correct installation can be verified by validating the software version in the following menu: “Config -> Select Device -> Verify”
ACUSON SC2000™ ultrasound system 4: Version 4.x less than 4.0E (VB10E) without US010/17S	Install US010/17S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “System Config Button-> System Settings > Service”

ACUSON SC2000™ ultrasound system 5: Version 5.0A (VB20A) without US011/17/S	Install US011/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “System Config Button-> System Settings > Service”
ACUSON X700™ ultrasound system 1.0: All versions V1.0 without US013/17/S	Install US013/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “Preset -> Select Device -> Verify”
ACUSON X700™ ultrasound system 1.1: All versions V1.1 without US014/17/S	Install US014/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “Preset -> Select Device -> Verify”
syngo® SC2000™ Workplace 4: Version 4.x less than 4.0E (VB10E) without US010/17/S	Install US010/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “Configuration Icon -> User Configuration -> System Settings > Service”
syngo® SC2000™ Workplace 5: Version 5.0A (VB20A) without US011/17/S	Install US011/17/S Please contact customer service. The correct installation can be verified by validating the software version in the following menu: “Configuration Icon -> User Configuration -> System Settings > Service”

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- 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 reestablishment of system operations.

GENERAL SECURITY RECOMMENDATIONS

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.

PRODUCT DESCRIPTION

Siemens Healthineers ACUSON SC2000 ultrasound systems and *syngo* Workplace products are used in clinical environments as connected or stand-alone devices for ultrasound imaging and image review purposes, respectively.

Siemens Healthineers ACUSON X700 ultrasound systems are used in clinical environments as connected or stand-alone devices for ultrasound imaging purposes.

Siemens Healthineers ACUSON P500 ultrasound systems and ACUSON P300 ultrasound systems are used as portable devices in clinical or point-of-care environments for ultrasound imaging purposes.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://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 defined by the customer to accomplish final scoring.

Vulnerability CVE-2017-0143

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

CVSS v3.0 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 CVE-2017-0144

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

CVSS v3.0 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 CVE-2017-0145

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

CVSS v3.0 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 CVE-2017-0146

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

CVSS v3.0 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 CVE-2017-0147

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

CVSS v3.0 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 CVE-2017-0148

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

CVSS v3.0 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

ADDITIONAL INFORMATION

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 (2017-05-22):	Publication Date
V1.1 (2017-06-01):	Added update information
V1.2 (2017-06-14):	Added information on Remote Update Handling (RUH)
V1.3 (2018-02-22):	Added update for P300

TERMS OF USE