SSA-492736: SMBv1 Vulnerabilities in Radiography, Mobile X-ray and Mammography 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

Some Radiography, Mobile X-ray and Mammography 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

- Mammomat Inspiration®: All versions without XP009/17/S

- Mammomat Fusion®: All versions without XP009/17/S

- *syngo*® MammoReport: All versions without XP009/17/S

- Mammomat Novation: All versions

- AXIOM® Aristos FX/MX/VX/TX: All versions without XP009/17/S

- MULTIX® M: All versions without XP009/17/S

- MULTIX® Swing mFD: All versions without XP009/17/S

- Mobilett XP digital®: All versions without XP009/17/S

DESCRIPTION

Siemens Healthineers Radiography, Mobile X-ray and Mammography systems are used in clinical environments for medical imaging using X-ray.

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 the XP009/17/S security update for the following software versions of the affected devices:

- Mammomat Inspiration® VB21 upwards

- Mammomat Fusion® VB50 upwards

- *syngo*® MammoReport VB24D upwards

- AXIOM® Aristos FX/MX/VX/TX with VB21D (XP052/13/R necessary)

- MULTIX® / Vertix® M VA30/VA40 (XP008/10/R necessary)

- MULTIX® Swing mFD: VA40 (XP008/10/R necessary)

- Mobilett XP digital® (XP036/13/R necessary)

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.

Until patches can be applied by customer service and for end-of-support products, Siemens Healthineers recommends isolating the 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 (2017-06-01):   Added update information
V1.2 (2017-06-14):   Added information on Remote Update Handling (RUH)

DISCLAIMER

See: https://www.siemens.com/terms_of_use