SSA-822184: Microsoft Web Server and HP Client Automation Vulnerabilities in Molecular Imaging Products from Siemens Healthineers

Publication Date 2017-07-26
Last Update 2017-07-26
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

Select Molecular Imaging products from Siemens Healthineers are affected by select Microsoft Windows 7 and HP Client Automation vulnerabilities. The exploitability of the vulnerabilities depends on the actual configuration and deployment environment of each product.

Siemens is working on updates for affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS

- Siemens PET/CT Systems: All Windows 7-based versions
- Siemens SPECT/CT Systems: All Windows 7-based versions
- Siemens SPECT Systems: All Windows 7-based versions
- Siemens SPECT Workplaces / Symbia.net: All Windows 7-based versions

The operating system of the Molecular Imaging products is displayed during boot up of the device.

Please contact local service contacts [1] if support is required to determine whether a specific product version is affected.

DESCRIPTION

Siemens Healthineers Molecular Imaging products are used in clinical environments for diagnostic imaging purposes.

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-2015-1635)

An unauthenticated remote attacker could execute arbitrary code by sending specially crafted HTTP requests to the Microsoft web server (port 80/tcp and port 443/tcp) of affected devices.

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:P/RL:T/RC:C

Vulnerability 2 (CVE-2015-1497)

An unauthenticated remote attacker could execute arbitrary code by sending a specially crafted request to the HP Client automation service on port 3465/tcp of affected devices.

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:P/RL:T/RC:C

Vulnerability 3 (CVE-2015-7860)

An unauthenticated remote attacker could execute arbitrary code by sending a specially crafted request to the HP Client automation service of affected devices.

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:P/RL:T/RC:C

Vulnerability 4 (CVE-2015-7861)

An unauthenticated remote attacker could execute arbitrary code by sending a specially crafted request to the HP Client automation service of affected devices.

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:P/RL:T/RC:C

SOLUTION

Siemens Healthineers is preparing updates for the affected products and recommends protecting network access to the Molecular Imaging products with appropriate mechanisms. It is advised to run the devices in a dedicated network segment and protected IT environment.

If the above cannot be implemented we recommend the following:

- If patient safety and treatment is not at risk, disconnect the 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] Local service contact numbers:
- America: 1-800-888-7436
- Europe, Middle East, and Africa: +49 9131 940 4000
- Asia and Australia: +86 (21) 3811 2121

[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 (2017-07-26): Publication Date

DISCLAIMER

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

