ADVISORY : MULTIPLE VULNERABILITES IN SIEMENS MOLECULAR IMAGING DEVICES (PET/CT SYSTEMS/X-RAY)

Reference: CERT.be Advisory #2017-005
Version: 1.0

Target audience: hospitals, medical centers, dentists etc who have Windows 7-based versions of SIEMENS PET / CT and SPECT / CT

Affected software: All Windows 7-based versions of Siemens PET/CT/SPECT Systems, All Windows 7 SPECT Workplaces / Sybmia.net, Mobilett Mira Max: All versions before VE10S without XP009/17/S
Type: Arbitrary code execution

Sources

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-822184.pdf
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-131263.pdf

Risks

Successful exploitation of these vulnerabilities may allow the attacker to remotely execute arbitrary code, that could allow full control of the system. (eg. Steal, modify patient information, change configuration,..)

These vulnerabilities have been assigned a CVSS v3 score of 9.8 out of 10. However impact to organizations depends on many factors that are unique to each organization.

Summary

Siemens has identified multiple vulnerabilities in Siemens Molecular Imaging Products running on Windows 7. Additionally Siemens is also alerting that multiple vulnerabilities have been identified in their Mobilett Mira Max – digital mobile X-ray machine.

These vulnerabilities can be exploited remotely, exploits that target these vulnerabilities are publicly available and require a minimal amount of effort.

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
- Mobilett Mira Max: All versions before VE10S without XP009/17/S

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

For the CT/PET/SPECT devices running windows 7 :

Vulnerability 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.

Vulnerability 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.

Vulnerability CVE-2015-7860 / 7861:

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

For the Mobilett Mira Max devices :

Vulnerability CVE-2017-0143 / 0144 / 0145 / 0146 / 0147 / 0148:

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

Recommended action

For the CT/PET/SPECT devices running windows 7 :

Siemens is preparing updates for the affected products and recommends protecting the network access to the Molecular Imaging products with appropriate measures.

While these updates haven't been released its advised by Siemens to run the devices in a dedicated network segment and a protected IT Environment.

For the Mobilett Mira Max: All versions before VE10S without XP009/17/S :

Siemens provides software update XP009/17/S for supported versions of Mobilett Mira Max before VE10S.

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 Siemens Customer service.

Until patches are available and for end-of-support products, Siemens 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 this is not possible, Siemens recommends 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 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.

In addition, Siemens recommends:

- Ensure you have appropriate backups and system restoration procedures.

- For specific patch and remediation guidance information contact your local Siemens Customer Service Engineer or a Regional Support Center.

CERT.be recommends that organisations take defensive measures to minimize the risk, specifically:

- Minimize network exposure for all medical devices and/or systems, and ensure that they are not accessible from the Internet.

- Locate all medical devices and remote devices behind firewalls, and isolate them from the business network.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

References

For more information on these vulnerabilities and more detailed mitigation instructions, please see Siemens Security Advisory SSA-814457 / 131263 at the following location:

http://www.siemens.com/cert/advisories