Siemens Healthcare GmbH, HC AT IR MK, Siemensstr. 1, 91301 Forchheim

Name Adrian Cronin
Department HC
E-mail adrian.cronin@siemens-healthineers.com

Date Jul 25, 2017

To all users of Artis systems, X-Workplace, Sensis and Arcadis systems with obsolete Hardware or Software

Important Safety Notice: **AX047/17/S**

Information about a potential vulnerability within the Microsoft Windows operating system of Artis, X-Workplace, Sensis and Arcadis systems.

Dear Customer,

This letter is to inform you about a potential safety-relevant security problem with possible hazard to patients.

What is the underlying issue and when does it occur?

The Artis, X-Workplace, Sensis and Arcadis systems utilize the operating systems Windows XP and Windows 7. A vulnerability of these operating systems is base for an acute hazard.
A malicious software, known as “WannaCry”-virus is targeting this vulnerability to invade susceptible systems and corrupt data on these systems by encryption.

Please find more technical information on the Siemens Internet representation:
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-023589.pdf

What is the impact on system operation and what is the potential risk?

The malicious software is encrypting data on affected systems. If parts of the Artis system, the X-Workplace, the Sensis or the Arcadis system are being encrypted, it could result in a situation in which it is necessary to cancel or restart clinical treatment or transfer it to a functioning system.
As an indirect effect, also loss of previously acquired data might be possible.

What action can you take?

The exploitability of any such vulnerability depends on the actual configuration and deployment environment of each product. According to Microsoft this ransomware spreads either by attachments/links in phishing emails or on malicious websites ("system zero infection") or via an infected system that exploits a vulnerability in a Windows component used in the context of open file shares of other systems reachable on the same network. Certain details may be found on the following Microsoft page:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

We would like to point out that neither the use of an email client nor browsing the internet is part of the intended use of most of the product types.

– **Recommendations**

The systems addressed by this letter and detailed in the following paragraph have an obsolete status of hardware or software.
For the following systems no Microsoft Patch can be deployed.

Arcadis:

Arcadis Varic	(P/N 8080017)
Arcadis Orbic	(P/N 8081080)
Arcadis Avantic	(P/N 10048590)
Arcadis Varic Gen2	(P/N 10143406) prior to S/N 15000
Arcadis Orbic Gen2	(P/N 10143407) prior to S/N 23000
Arcadis Avantic Gen2	(P/N 10143408) prior to S/N 33000

syngo X-WP:

X-Leonardo	VA70, VA71, VA72, VB11A/B, VB11M,

Above products are listening on network ports 139/tcp, 445/tcp or 3389/tcp.
Their exploitation exposure depends on the security measures within the network.
In order to protect a vulnerable product from exploitation it should be isolated from any potentially infected system within its respective network segment (e.g. product deployed in a network segment separated by firewall control blocking access to network ports 139/tcp, 445/tcp and 3389/tcp).

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.

For following systems we recommend upgrading the obsolete system software to an up to date version for which a Microsoft Patch can be deployed:

Artis:

AXIOM Artis	VB22N, VB23D/F/G/H/J	➔ please update to VB23P
AXIOM Artis	VB30C/E, VB31E/F, VB35A	➔ please update to VB35E
Artis zee	VC13A/B, VC13D/E, VC14B/D/E/G	➔ please update to VC14J
Artis zee	VC21A	➔ please update to VC21C
Artis One	VA10B, VA10C	➔ please update to VA10D

syngo X-WP:

syngo X-WP	VB13E	➔ please update to VB13F
syngo X-WP	VB14A, VB14B	➔ please update to VB14C
syngo X-WP	VB15B, VB15C	➔ please update to VB15D
syngo X-WP	VB20B, VB20C	➔ please update to VB20D
syngo X-WP	VB21B	➔ please update to VB21C
syngo X-WP	VC10C	➔ please update to VC10D

Sensis:

Sensis	VC03A/B/C/D	➔ please update to VC03G or later
Sensis	VC10B/C, VC11A/B/C	➔ please update to VC11D or later
Sensis	VC12A	➔ please update to VC12C or later
Sensis	VC12K	➔ please update to VC12L or later

In addition, Siemens Healthineers recommends:
Ensure you have appropriate backups and system restoration procedures.

How was the issue detected?

The threat was identified when the infection of certain private, industrial and healthcare equipment was reported. An according vulnerability of Artis, X-Workplace, Sensis and Arcadis systems has to be assumed.

What risks are there for patients who have previously been examined or treated using this system?

We do not consider it necessary to re-examine any patients in this case. This is a possible defect that had no influence on the treatment of patients.

We thank you for your cooperation in dealing with this customer safety notice, and request that you promptly notify and instruct accordingly all the staff at your organization who need to be aware of this problem. Please forward this safety information to any other organizations that could be affected by this measure.

If the device has been sold and is therefore no longer in your possession, please forward this safety notice to the new owner. We would also request you to inform us of the identity of the device's new owner where possible.

Best regards,

Ronan Kirby
Head of Service Ireland

Adrian Cronin
Service Supervisor AX/XP ROI