INFORME DE SEGURIDAD

DIRECCIÓN DE DISPOSITIVOS MÉDICOS Y OTRAS TECNOLOGÍAS

El INVIMA informa a los usuarios en general que el Grupo de Tecnovigilancia ha emitido una comunicación relacionada con un Informe de Seguridad asociado a:

NOMBRE DEL DISPOSITIVO MÉDICO	Sistema para Angiografía AXIOM ARTIS SIEMENS
NO. IDENTIFICACIÓN RISARH	I1708-331
REFERENCIAS DEL DISPOSITIVO MEDICO	ARCADIS, ARTIS, SENSIS, SYNGO X – WORKPLACE, versiones de software específicas.
REGISTRO SANITARIO	2008EBC-0001426
INDICACIONES Y USO ESTABLECIDOS	Equipo para diagnóstico por imagen.
NOMBRE DEL FABRICANTE	Siemens Shenzhen Magnetic Resonance Ltd. Siemens Healthcare Gmbh Siemens A.G.
DESCRIPCION DEL PROBLEMA	El fabricante establece que los equipos anteriores utilizan sistemas operativos Windows XP y Windows 7 donde una vulnerabilidad de estos sistemas operativos es la base para un potencial peligro, pues afirma que un software malicioso conocido como "WannaCry" virus que está dirigido a esta vulnerabilidad podria invadir los sistemas susceptibles y afectar los datos en estos sistemas de cifrado, Siemens también afirma que según Microsoft, este ransomware se propaga por archivos adjuntos / enlaces en correos electrónicos de phishing o en sitios web maliciosos (infección por el sistema cero) o de un sistema infectado que explota una vulnerabilidad en un componente de Windows utilizado en el contexto de abrir archivos compartidos de otros sistemas accesibles en la misma red, conllevando a que se presenten eventos adversos sobre los pacientes por confusión en la identificación de resultados o perdida de los mismos.
FUENTE	ANEXO
FECHA DE NOTIFICACION	01 de Agosto de 2017

INFORME DE SEGURIDAD

DIRECCIÓN DE DISPOSITIVOS MÉDICOS Y OTRAS TECNOLOGÍAS

RECOMENDACIÓN:

En caso de identificar la existencia del producto mencionado anteriormente comuníquese con su proveedor quien determinara las acciones que se llevaran a cabo.

Es importante mantener un estado de alerta, realizando un seguimiento permanente a los productos que se fabrican y/o comercializan en el país, divulgando la información de seguridad respectiva entre los profesionales de la salud que realizan uso de estos recursos tecnológicos.

Para mayor información comuníquese al teléfono 2948700 extensión 3880 en Bogotá, ó al correo electrónico tecnovigilancia@invima.gov.co

INFORME DE SEGURIDAD

DIRECCIÓN DE DISPOSITIVOS MÉDICOS Y OTRAS TECNOLOGÍAS

ANEXO

[High Priority] - A28925 : Siemens—Artis, syngo X-Workplace, Sensis, and Arcadis Systems: Manufacturer Responds to WannaCry Ransomware Vulnerabilities
Medical Device Ongoing Action

Published: Thursday, July 27, 2017

UMDNS Terms:

- Radiographic Systems [18429]

Product Identifier:
Systems: (1) Arcadis, (2) Artis, (3) Sensis, (4) syngo X-Workplace (X-WP) *[Capital Equipment]*

Systems for Which No Microsoft Patch Can Be Deployed:	Part Nos.:	Software Versions:
Arcadis Avantic	10048590	Not listed
Arcadis Orbic	8081080	Not listed
Arcadis Varic	8080017	Not listed
Arcadis Avantic Generation 2	10143408 (serial numbers 33000 and below)	Not listed
Arcadis Orbic Generation 2	10143407 (serial numbers 23000 and below)	Not listed
Arcadis Varic Generation 2	10143406 (serial numbers 15000 and below)	Not listed
syngo X-WP X-Leonardo	Not listed	VA70, VA71, VA72, VB11A/B, VB11M

Systems with Obsolete Software Versions Which Can Be Updated for Microsoft Patch Deployment:	Obsolete Software Versions:	Recommended Update Software Version:
Artis AXIOM	VB22N, VB23D/F/G/H/J	VB23P
Artis AXIOM	VB30C/E, VB31E/F, VB35A	VB34E
Artis One	VA10B, VA10C	VA10D
Artis zee	VC13A/B, VC13D/E, VC14B/D/E/G	VC14J
Artis zee	VC21A	VC21C
Sensis	VC03A/B/C/D	VC03G or above
Sensis	VC10B/C, VC11A/B/C	VC11D or above
Sensis	VC12A	VC12C or above
Sensis	VC12K	VC12L or above
syngo X-WP	VB13E	VB13F
syngo X-WP	VB14A, VB14B	VB14C
syngo X-WP	VB15B, VB15C	VB15D

INFORME DE SEGURIDAD
DIRECCIÓN DE DISPOSITIVOS MÉDICOS Y OTRAS TECNOLOGÍAS

syngo X-WP	VB20B, VB20C	VB20D
syngo X-WP	VB21B	VB21C
syngo X-WP	VC10C	VC10D

Geographic Regions: (Impact in specific regions has not been identified or ruled out at the time of this posting), Worldwide

Manufacturer(s): Siemens Healthcare 40 Liberty Blvd, Malvern, PA, 19335, United States

Suggested Distribution: Clinical/Biomedical Engineering, Diagnostic Imaging, Information Technology

Problem:
In a June 28, 2017, Important Safety Notice letter submitted by an ECRI Institute member hospital and posted by the German Federal Institute for Drugs and Medical Devices (BfArM), Siemens states that the above systems utilize Windows XP and Windows 7 operating systems and that a vulnerability of these operating systems is base for an acute hazard. Siemens also states that a malicious software known as "WannaCry" virus is targeting this vulnerability to invade susceptible systems and corrupt data on these systems by encryption. Siemens further states that if parts of the above systems are 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, loss of previously acquired data may occur. The exploitability of any such vulnerability depends on the actual configuration and deployment environment of each product. Siemens also states that according to Microsoft, this ransomware spreads either by attachments/links in phishing e-mails or on malicious websites ("system zero infection") or from 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. For additional details on the WannaCry ransomware, see the Microsoft website . Siemens further states that neither the use of an e-mail client or browsing the internet is part of the intended use of most of the above products. The manufacturer has not confirmed the information provided in the source material.

Action Needed:
Identify any affected systems in your inventory. If you have affected systems, verify that you have received the June 28, 2017, Important Safety Notice letter from Siemens. Siemens states that the above systems for which no Microsoft patch can be deployed are listening on network ports 139/tcp, 445/tcp, or 3389/tcp, and that their exploitation exposure depends on the security measures within the network. To protect a vulnerable product from exploitation, it should be isolated from any potentially affected 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 this cannot be implemented, Siemens recommends that, if patient safety and treatment is not at risk, you disconnect the uninfected product from the network and use it in standalone mode. For the above systems with obsolete software that can be updated to a version for which a Microsoft patch can be deployed, Siemens recommends that you perform this upgrade. In addition, Siemens recommends that you ensure that you have appropriate backups and system restoration procedures. It is not necessary to re-examine patients treated with affected systems; this potential defect had no influence on the treatment of patients. Notify all relevant personnel at your facility of the information in the letter, and forward a copy of the letter to any facility to which you have further distributed affected systems and notify Siemens of the transfer.
For further Information:
Siemens
Website: Click here

References:

- Germany. Federal Institute for Drugs and Medical Devices. Urgent Field Safety Notice for Artis, X-Workplace, Sensis and ARCADIS systems by Siemens Healthcare GmbH; Business Area Advanced Therapies [online]. 2017 Jun 30 [cited 2017 Jul 20]. Available from Internet: Click here .

Comments:

- For information on other Siemens actions related to the WannaCry ransomware, see Alerts A28839 and A28842 .
- This alert is a living document and may be updated when ECRI Institute receives additional information. In circumstances in which we determine that it is appropriate for customers to repeat their review of an issue (e.g., when additional affected product has been identified), we will post a separate update alert. In other cases, we may add information, such as additional commentary, recommendations, and/or source documents, to the original alert. For additional information regarding the format of this alert, refer to our HDA Format Guide .

Source(s):

- 2017 Jul 26. Member Hospital. Siemens letter submitted by ECRI Institute member hospitals: AX047/17/S Download
- 2017 Jul 27. BfArM (Germany). 06287/17 Download
- 2017 Jul 27. BfArM (Germany). AX/047/17S Download