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 de Ultrasonido para Diagnostico SIEMENS
NO. IDENTIFICACIÓN RISARH	I1709-402
REFERENCIAS DEL DISPOSITIVO MEDICO	ACUSON, versiones de software VE10A, VC30, VC31, VD10.
REGISTRO SANITARIO	2008DM-0001867
INDICACIONES Y USO ESTABLECIDOS	Sistema de ultrasonido para aplicaciones de: abdomen, intraoperatorio, obstetricia y ginecología, pelvis, mama, ortopedia, urología, pequeñas partes, transcraneal, musculo esquelético, vascular, vascular periférico, cardiología, intracardiaca y transesofagia para pacientes neonatales, pediátricos y adultos.
NOMBRE DEL FABRICANTE	Siemens Medical Solutions Usa, Inc. Esaote S.P.A. Siemens Ltd. Seoul Siemens Ltd. Seoul
DESCRIPCION DEL PROBLEMA	El afirma que el sistema operativo Microsoft Windows en los sistemas anteriores tiene una vulnerabilidad al virus WannaCry, si la configuración del sistema ha sido respaldada y restaurada en cualquier momento, existe una alta probabilidad de que el sistema sea vulnerable al virus, lo cual puede detener la funcionalidad del sistema, en los dispositivos referenciados con las versiones de software VC30 y VC31, una pantalla azul en el sistema indica la probabilidad de que su red esté infectada, por su parte en la versión de software VD10 y VE10A, aún no se han recibido informes de infecciones pero el riesgo existe, conllevando a que se presenten incidentes o eventos adversos sobre los pacientes o retrasos en los procedimientos.
FUENTE	ANEXO
FECHA DE NOTIFICACION	06 de Septiembre 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] - A29148 : Siemens—ACUSON S Ultrasound Systems: Manufacturer Responds to WannaCry Ransomware Vulnerabilities
Medical Device Ongoing Action

Published: Thursday, August 31, 2017

UMDNS Terms:

- Scanning Systems, Ultrasonic [14278]

Product Identifier:
ACUSON S Ultrasound Systems *[Capital Equipment]*
Software Version VE10A and All Software Versions of the following Software Releases: VC30, VC31, VD10

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: Cardiology/Cardiac Catheterization Laboratory, Clinical/Biomedical Engineering, Obstetrics/Gynecology/Labor and Delivery, Diagnostic Imaging, Information Technology

Problem:
In a Customer Advisory Notification letter submitted by an ECRI Institute member hospital, Siemens states that the Microsoft Windows operating system on the above systems has a vulnerability to the WannaCry virus. Siemens also states that if the system settings have been backed up and restored at any time, there is a high probability that the system is vulnerable to the virus. Siemens further states that exposure to the virus may halt system functionality, potentially resulting in a delay in procedure for a sedated patient or necessitating reinsertion of a transesophageal transducer or catheter, or repeat of a stress echo exam. Siemens states that patient harm as a result of this virus is improbable. For the above systems with software releases VC30 and VC31, a blue screen on the system indicates the likelihood that your network is infected. For the above systems with software release VD10 or version VE10A, Siemens has received no reports of infections; however, if the network becomes infected, there is a high probability that the system will also become infected. 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 Customer Advisory Notification letter from Siemens. For systems with software releases VC30 and VC31, if you observe a blue screen, indicating that your network is infected, to continue to use the system you must disconnect the system from the infected network, restart the system, and then continue use of the system disconnected from the network. For affected systems with software release VD10 or version VE10A, if you observe symptoms of infection, such as lockups or ransomware messages, you must discontinue use of the system. Disconnect it from the network and contact your Siemens service representative. Siemens is initiating a product update to correct this vulnerability. For information on this update and others, click here and here . Notify all relevant personnel at your facility of the information in the letter.
For further Information:
Siemens customer care center
Website: Click here

Comments:

- For information on other Siemens action related to the WannaCry ransomware, see Alerts A28839 , A28842 , and A28925 .
- For information on a Siemens action related to Microsoft Windows 7 and HP Client Automation vulnerabilities on various molecular imaging products, see Alert A29058 .
- 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 .