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	Equipo para Electrocardiografía GE
NO. IDENTIFICACIÓN RISARH	I1806-383
REFERENCIAS DEL DISPOSITIVO MEDICO	MAC3500, MAC5500 y algunos servidores de dispositivos inalámbricos.
REGISTRO SANITARIO	2017DM-0001541-R1
INDICACIONES Y USO ESTABLECIDOS	Monitorizar parámetros clínicos a pacientes hospitalizados.
NOMBRE DEL FABRICANTE	Ge Medical Systems Technologies Co Ltd Carefusion Finland 320 Oy Ge Healthcare Finland Oy
DESCRIPCION DEL PROBLEMA	El fabricante informa que los sistemas anteriores pueden ser susceptibles a algunas vulnerabilidades de firmware, relacionadas con autenticación incorrecta, neutralización inadecuada de elementos especiales utilizados en los comandos del sistema operativo, parámetros de llamada del sistema que no se desinfecta correctamente, lo cual puede permitir la ejecución remota del código de los sistemas operativos, la anterior situación podría conllevar a que se presenten potenciales violaciones de seguridad y por consiguiente posibles eventos adversos sobre los pacientes.
FUENTE	ANEXO
FECHA DE NOTIFICACION	13 de junio de 2018

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] - A30604 01 : GE/Silex: Various MAC ECG Systems and Wireless Device Servers: May Be Vulnerable to Improper Authentication and OS Command Injection [Update]
Medical Device Ongoing Action

Published: Monday, June 4, 2018

UMDNS Terms:

- Information Systems, Data Management, Cardiology, Electrocardiography [22499]
- Network Servers [21973]

Product Identifier:
[Capital Equipment]

Product	GE Healthcare Model
Resting ECG Analysis Systems	MAC 3500, MAC 5000, MAC 5500, MAC 5500 HD
Wireless ECG Communication Modules	MobileLink

Product	Silex Technology Inc Model	Version
Wireless Device Servers	GEH-500	<= 1.54
	SX-500	All
	GEH-SD-320AN	<= GEH-1.1
	SD-320AN	<= 2.01

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

Manufacturer(s): GE Healthcare9900 Innovation Dr, Wauwatosa, WI 53226, United States
Silex Technology Inc167 West 7065 South, Midvale, UT 84047, United States

Suggested Distribution: Cardiology/Cardiac Catheterization Laboratory, Clinical/Biomedical Engineering, Critical Care, Emergency/Outpatient Services, Information Technology, EMS/Transport

Summary:
Update Reason: GE and Silex provide updated firmware image for the GEH-SD-320AN system. This Alert provides additional information based on a May 31, 2018, Advisory revision regarding Alert A30604 . The updated firmware image is available for download here .

Problem:
In a May 8, 2018, Advisory, the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) states that the above systems may be susceptible to the following vulnerabilities:

- Improper authentication (CWE-287)
  - Authentication is not verified when making certain POST requests, which may allow attackers to modify system settings.
- Improper neutralization of special elements used in an OS command (OS Command Injection) (CWE-78)
  - A system call parameter is not properly sanitized, which may allow remote code execution.

The manufacturers have not confirmed the information provided in the source material.

Action Needed:
The following actions are those listed in Alert A30604 . Identify any affected systems in your inventory. If you have affected systems, verify that you have reviewed the May 8, 2018, ICS-CERT Advisory . GE and Silex recommend the following mitigations:

- For MobileLink and SX-500 systems, enable the "update" account within the web interface, which is not enabled by default. Set the secondary password for the "update" account to prevent unauthenticated changes to the device configuration.
- For MobileLink and GEH-SD-320AN systems, Silex Technology and GE Healthcare have produced an updated firmware image for the GEH-SD-320AN system, which will be made available for download from GE upon completion of testing.

GE will post information pertaining to enabling the "update" account and download of new firmware here . The firmware update for SD-320AN is separate from GEH-SD-320AN and will be available for download from Silex Technology at a future date. This update does not pertain to the listed GEH device. Contact Silex Technology for more information regarding download and application of this new firmware. National Cybersecurity and Communications Integration Center (NCCIC) recommends the following actions to minimize the risk of exploitation of these vulnerabilities:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks 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 a VPN is only as secure as the connected

devices.

Perform proper impact analysis and risk assessment before deploying these defensive measures. Additional mitigation guidance and recommended practices are publicly available in the NCCIC Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies , which is available for download from the ICS-CERT website . NCCIC also provides a section for control systems security recommended practices . Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies .

For Further Information:
NCCIC
E-mail: NCCICCUSTOMERSERVICE@hq.dhs.gov
Tel.: (888) 282-0870
Website: Click here
GE
Website: Click here
Silex
Website: Click here

References:
United States:

- Department of Homeland Security. Industrial Control Systems Cyber Emergency Response Team. Advisory. Silex Technology SX-500/SD-320AN or GE Healthcare MobileLink [online]. 2018 May 8 [cited 2018 May 14]. Available from Internet: Click here .
- Department of Homeland Security. Industrial Control Systems Cyber Emergency Response Team. Advisory. Silex Technology SX-500/SD-320AN or GE Healthcare MobileLink (Update A) [online]. 2018 May 31 [cited 2018 Jun 1]. Available from Internet: Click here .

Comments:

- 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):

- 2018 Jun 1. ICS-CERT Advisory: ICSMA-18-128-01 Download