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	Electroencefalógrafo NATUS
NO. IDENTIFICACIÓN RISARH	I1806-425
REFERENCIAS DEL DISPOSITIVO MEDICO	Referente al software XLTEK NEURO WORKS Versión 8
REGISTRO SANITARIO	2009DM-0003394
INDICACIONES Y USO ESTABLECIDOS	Indicado para el registro de señales electroencefalograficas y polisomnograficos para investigación o uso clínico.
NOMBRE DEL FABRICANTE	Bio-Logic Systems Corp Excel Tech Limited Natus Medical Incorporated (Incorporated Dba Excel Tech Limeted)
DESCRIPCION DEL PROBLEMA	El fabricante informa que la versión del software referenciada puede ser vulnerable al desbordamiento del búfer basado en pila y la lectura fuera de límites, la explotación exitosa de estas vulnerabilidades requiere acceso a la red de clientes de NATUS, y podría bloquear el dispositivo al que se accede; una condición de desbordamiento del búfer puede permitir la ejecución remota de código, la anterior situación podría conllevar a que se presenten retrasos en los procedimientos y potenciales eventos adversos sobre los pacientes.
FUENTE	ANEXO
FECHA DE NOTIFICACION	29 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] - A30849 : Natus—Xltek NeuroWorks Software: May Be Susceptible to Cybersecurity Vulnerabilities
Medical Device Ongoing Action

Published: Tuesday, June 19, 2018

UMDNS Terms:

- Software, Physiologic Monitoring, Electroencephalography [26714]

Product Identifier:
[Capital Equipment]

Product	Natus Medical Inc Model	Software Version
Electroencephalography (EEG) System Software	Xltek NeuroWorks	8

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

Manufacturer(s): Natus Medical Inc 6701 Koll Center Pkwy, Pleasanton, CA 94566, United States

Suggested Distribution: Clinical/Biomedical Engineering, Critical Care, Information Technology, Neurology, Sleep Laboratory

Problem:
In a June 14, 2018, Advisory, the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) states that the above software may be vulnerable to Stack-Based Buffer Overflow and Out-of-Bounds Read. ICS-CERT also states that successful exploitation of these vulnerabilities require access to the Natus customer network, and could crash the device being accessed; a buffer overflow condition may allow remote code execution. The potential vulnerabilities are as follows:

- Out-of-Bounds Read (CWE-125)
  - A specially-crafted packet may be able to cause an out-of-bounds read, which may result in a denial-of-service condition.
- Stack-Based Buffer Overflow (CWE-121)
  - An attacker may cause a buffer overflow by sending a specially-crafted packet to the affected product while the product attempts to open a file requested by the client.
  - A specially-crafted packet received during the execution of certain commands can cause memory to be overwritten in a way that could allow an attacker to take control of the program.
  - An error in the way the program parses data structures may allow an attacker to take control of the system by sending it a specially-crafted packet.
  - A specially-crafted packet takes advantage of the way the program parses data structures and may cause a buffer overflow, which may allow remote execution of arbitrary code.

The manufacturer has not confirmed the information provided in the source material.

Action Needed:
Identify any affected software in your inventory. If you have affected software, verify that you have reviewed the June 14, 2018, ICS-CERT Advisory . Natus recommends installation of NeuroWorks/SleepWorks 8.5 GMA 3, a software update with security enhancements to address the vulnerabilities identified in NeuroWorks/SleepWorks 8. A free software update to NeuroWorks/SleepWorks 8.5 GMA 3 is available to users using NeuroWorks/SleepWorks Version 8.0, 8.1, 8.4, or 8.5. Natus recommends installing this update on affected systems as quickly as possible.
The National Cybersecurity and Communications Integration Center (NCCIC) recommends that users take defensive measures to minimize the risk of exploitation of the above vulnerabilities. Users should:

- 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. Recognize that VPN is only as secure as the connected devices.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies .
For Further Information:
NCCIC
Tel.: (888) 282-0870
E-mail: NCCICCUSTOMERSERVICE@hq.dhs.gov
Website: Click here
Natus
Website: Click here
References:

- United States. Department of Homeland Security. Industrial Control Systems Cyber Emergency Response Team. Advisory. Natus Xltek NeuroWorks [online]. 2018 Jun 14 [cited 2018 Jun 19]. 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 19. Member Hospital. ICS-CERT Advisory Download