OVERVIEW

Neuwave Medical has assessed vulnerabilities associated with recent WannaCrypt or WannaCry ransomware attacks in Neuwave's Certus® system. Existing mitigations will prevent exploitation of the vulnerabilities used in those attacks. Although there is no immediate risk identified, Neuwave will continue to monitor threats to our devices and will release patches as necessary.

AFFECTED PRODUCTS

Certus®140 System

Certus®140 System with Ablation Confirmation

IMPACT

With existing mitigations in place there is no impact identified. The Certus® 140 System utilizes a software firewall to prevent SMB inbound traffic that fully mitigates SMBv1 vulnerabilities. The Certus® 140 System also utilizes software whitelisting as an additional security measure to protect against vulnerabilities and cybersecurity threats like WannaCrypt.

Background

Neuwave Medical is a part of the Ethicon family of companies. The affected product, the Certus®140 Microwave Ablation System (the "System"), is indicated for the ablation (coagulation) of soft tissue in percutaneous, open surgical and in conjunction with laparoscopic surgical settings. The System is not indicated for use in cardiac procedures. The System is designed for facility use and should only be used under the orders of a clinician.

VULNERABILITY CHARACTERIZATION

Vulnerability Overview

The vulnerabilities used in recent WannaCrypt or WannaCry ransomware attacks have been assessed for mitigation including:

- SMBv1 Vulnerability 1 CVE-2017-0143
- SMBv1 Vulnerability 2 CVE-2017-0144
- SMBv1 Vulnerability 3 CVE-2017-0145
- SMBv1 Vulnerability 4 CVE-2017-0146
- SMBv1 Vulnerability 5 CVE-2017-0147
- SMBv1 Vulnerability 6 CVE-2017-0148

VULNERABILITY DETAILS

Exploitability

These vulnerabilities cannot be exploited remotely due to existing mitigations.

Existence of Exploit

Exploit code is available, but prevented by existing mitigations.

Difficulty

An attacker must first utilize restricted, local access on the Certus® 140 device to disable the software firewall and whitelisting before there is an ability to exploit these vulnerabilities.

MITIGATION

The Certus® 140 System utilizes a software firewall and software whitelisting that prevents vulnerabilities related to the recent WannaCrypt ransomware. Neuwave Medical applies required core operating system patches in each version of our product releases that will fully close the operating system deficiencies. Customers will be notified upon release of our next update.

- If customers are concerned a Certus®140 system has been impacted by a Cyber-attack, please immediately disconnect the system from the network and contact a service technician and/or productsecurity@its.jnj.com.