OVERVIEW

Biosense Webster, Inc (BWI) has identified vulnerabilities with existing mitigations in BWI's Carto®3 system associated with SMBv1 as used in recent Wannacry ransomware attacks. BWI is developing a cybersecurity update to address these vulnerabilities. Mitigating controls for customers are already in place for current supported versions (V3 and V4) of the Carto®3 system. Older versions of the Carto®3 system (Windows XP-based) are vulnerable.

AFFECTED PRODUCTS

Carto®3 System V2 and below

IMPACT

Successful exploitation of unmitigated vulnerabilities in V2 (Windows XP-based) of the Carto®3 system may allow an attacker to remotely access the device and upload a payload for execution (e.g. Ransomware). The impact associated with the successful exploitation of these vulnerabilities would not have an impact on patient safety.

Background

The affected product, the Carto®3 System is an advanced imaging technology that uses electromagnetic technology to create real-time three-dimensional (3D) maps of a patient's cardiac structures. The system is designed to help electrophysiologists navigate the heart by generating an accurate 3D map, as well as pinpointing the exact location and orientation of catheters in the heart during diagnostic and therapeutic procedures for patients suffering from heart rhythm conditions (cardiac arrhythmias).

VULNERABILITY CHARACTERIZATION

Vulnerability Overview

SMBv1 Vulnerability 1 CVE-2017-0143

The SMBv1 server in Microsoft Windows 7 SP1 allows remote attackers to execute arbitrary code via crafted packets.

CVE-2017-0143 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

SMBv1 Vulnerability 2 CVE-2017-0144

The SMBv1 server in Microsoft Windows7 SP1 allows remote attackers to execute arbitrary code via crafted packets.

CVE-2017-0144 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

SNBv1 Vulnerability 3 CVE-2017-0145

The SMBv1 server in Microsoft Windows7 SP1 allows remote attackers to execute arbitrary code via crafted packets.

CVE-2017-0145 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

SMBv1 Vulnerability 4 CVE-2017-0146

The SMBv1 server in Microsoft Windows7 SP1 allows remote attackers to execute arbitrary code via crafted packets.

CVE-2017-0146 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

SMBv1 Vulnerability 5 CVE-2017-0147

The SMBv1 server in Microsoft Windows7 SP1 allows remote attackers to obtain sensitive information from process memory via crafted packets.

CVE-2017-0147 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

SMBv1 Vulnerability 6 CVE-2017-0148

The SMBv1 server in Microsoft Windows7 SP1 allows remote attackers to execute arbitrary code via crafted packets.

CVE-2017-0148 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been assigned; the CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

VULNERABILITY DETAILS

Exploitability

These vulnerabilities could be exploited remotely.

Existence of Exploit

Exploit code is available.

Difficulty

An attacker with low skill would be able to exploit these vulnerabilities.

MITIGATION

BWI is developing a cybersecurity update to address these vulnerabilities and has issued mitigation controls for customers.

- The latest Carto®3 System is deployed with the Windows Firewall enabled by default, blocking all SMB ports (137, 138, 139, 445).
- BWI recommends customers refer to the Carto®3 Instructions for Use (IFU) around Backing Up, Restoring and Deleting Studies.
- If customers are concerned a Carto®3 system has been impacted by a Cyber-attack, please take the following actions:
    - Disconnect the system from the network
    - Disconnect all other point-to-point connected machines
    - Contact a service technician and/or productsecurity@its.jnj.com.