OVERVIEW

Biosense Webster, Inc. (BWI) identified a controlled security risk in the CARTO® 3 System related to the recently published DICOM (Digital Imaging and Communications in Medicine) vulnerability (CVE-2019-11687). This vulnerability is in the preamble defined by the DICOM File format which could allow DICOM files to be stored on media with executable malware inserted.

Existing security controls associated with the CARTO® 3 System prevent exploitation of this vulnerability.

PRODUCTS ASSESSED FOR CVE-2019-11687

CARTO® 3 V6

IMPACT

CARTO® 3 V6 is not affected by this vulnerability as the CARTO® 3 V6 software performs input validation when importing DICOM files. Functionality, design and intended use of CARTO® 3 System is not impacted.

Even if the preamble contains malicious code, since CARTO® 3 V6 ignores it, the malicious code in the preamble cannot cause any unexpected behavior in CARTO® 3 System.

The security controls in place lower the risk of this vulnerability to a controlled level.

Background

The assessed product, the CARTO® 3 V6 System, is an advanced imaging device 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

Recently published DICOM (Digital Imaging and Communications in Medicine) vulnerability has been assessed for mitigation. The DICOM standard is the international standard to transmit, store, retrieve, print, process, and display medical imaging information. This vulnerability is in the preamble defined by the DICOM File format and has been identified as CVE-2019-11687. It could allow DICOM files stored on media to have executable malware inserted.

VULNERABILITY DETAILS

Exploitability

- The CARTO® 3 V6 workstation does input validation before DICOM file is imported into the system, and in any case, discards the DICOM preamble.
  It reads and displays a DICOM file after the import. It does not execute the DICOM file.

- For exploit to work, malicious actor requires physical access to the device, access to the operating system to transfer the “infected DICOM file” to the device and rights to execute the infected file on the device.
  Carto3 System has following security controls in place which reduce the likelihood of this exploit:
  - CARTO3 V6 workstation has restricted physical access (ensured by the hospital)
  - Access to the Operating System and ability to execute any file on the system is protected through OS hardening and limited user access control.

Difficulty

An attacker must first utilize restricted, local access on the CARTO® 3 V6 device and access the operating system to transfer and execute the infected DICOM before there is an ability to exploit this vulnerability.

MITIGATIONS

Not Applicable. Existing security controls associated with the CARTO® 3 System prevent exploitation of this vulnerability.

RECOMMENDATIONS

None necessary.

If customers are concerned that a CARTO® 3 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.

CHANGE HISTORY

July 23, 2019: Date Created.

Aug 5, 2019: Date Last Modified. Minor addition to “Mitigations” and “Recommendations” section.