OVERVIEW

Biosense Webster, Inc. (BWI) identified a controlled security risk in the CARTO® 3 System related to the operating system vulnerability (CVE-2019-0708), which was announced by Microsoft on May 14, 2019. This vulnerability affects systems that use remote desktop services on Windows XP, Windows 7, Windows 2003 and Windows 2008. To address this vulnerability, Microsoft has released a patch along with security guidance on mitigations/workarounds.

Existing mitigations associated with the CARTO® 3 System will prevent exploitation of this vulnerability. Although there is no immediate risk identified, BWI will deliver the patch for vulnerability CVE-2019-0708 as part of the next periodical service pack for CARTO® 3 install base. BWI will continue to monitor threats to our devices and will release patches as necessary.

PRODUCTS ASSESSED FOR CVE-2019-0708

CARTO® 3 V6

IMPACT

With existing mitigations in place there is no impact identified.

Mitigation and control on CARTO® 3 V6 are implemented in the following way:

- The CARTO® 3 V6 workstation can be used as standalone system and does not need to be connected to the local network for medical use. It has no Internet connection. Device can optionally be connected to the hospital network for DICOM and PACS connectivity, but Remote Desktop Services are disabled on the device by default and not utilized.
- The CARTO® 3 V6 workstation has RDP services (Remote Desktop Protocol) disabled. No administrative or user remote-control session is foreseen.
- Windows firewall settings prevent connections to the standard RDP port and services.

The 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

Remote Desktop Services remote code execution vulnerability (CVE-2019-0708), which was announced by Microsoft on May 14, 2019 has been assessed for mitigation. This vulnerability affects systems that use remote desktop services on Windows XP, Windows 7, Windows 2003 and Windows 2008.

VULNERABILITY DETAILS

Exploitability

This vulnerability cannot be exploited remotely due to existing mitigations.

Difficulty

An attacker must first utilize restricted, local access on the CARTO® 3 V6 device to disable the software firewall besides enabling Remote Desktop Services before there is an ability to exploit this vulnerability.

MITIGATION

CARTO® 3 V6 utilizes a software firewall to restrict network interface and has remote desktop services disabled by default which mitigates the vulnerability.

Biosense Webster plans to deliver the patch for vulnerability CVE-2019-0708 as part of the next periodical service pack for CARTO® 3 install base, together with other security patches that will be available at the time of its preparation.

The latest released CARTO® 3 V6 version V6Phase7 and the next version V6SP2 being released in June 2019 do not include the Microsoft update released for CVE-2019-0708 (RDP vulnerability) along with recent Windows updates.

- 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

May 31, 2019: Original Security Advisory published
June 7, 2019: Revised Section “Difficulty”