OVERVIEW

On May 14, 2019, Microsoft announced Remote Code Execution Vulnerability-CVE-2019-0708 in Remote Desktop Services. This vulnerability affects systems that use remote desktop services on Windows XP, Windows 7, Windows 2003 and Windows 2008.

AFFECTED PRODUCTS

Product Name	Product Version
Brainlab® Curve	15700 / 15705 Curve Ceiling Mount
Brainlab® Kick	18083 - Kick® 1.2
Brainlab® Kick	18090 - Kick® 1.1 / 1.3
Brainlab® Kick	18070 - Kick® 1.0 / 1.3

IMPACT

Products and versions specified above are affected by this vulnerability.

Background

Brainlab's Kick® System is a computer-aided surgical navigation system using optical tracking to assist surgeons during surgical procedures.

Brainlab's Curve® System is a command and control center for image-guided surgery.

DePuy Synthes is a distributor of the Brainlab Curve® System and Brainlab Kick® System.

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 Brainlab Kick and Curve Systems.

VULNERABILITY DETAILS

Exploitability

This vulnerability can be exploited remotely if remote desktop services are enabled.

Difficulty

Attack Complexity is low.

Security Updates

Security Guidance and downloads Link
To address this vulnerability, Microsoft has released a patch along with security guidance on mitigations/workarounds. Patches should be applied as per “Anti-Virus and Windows Update Policy” in the User Guide provided with Brainlab Systems.

Mitigations

Disable Remote Desktop Services if they are not required.

Workarounds

1. Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.

2. Block TCP port 3389 at the enterprise perimeter firewall.

Recommendations:

- Verify that the Microsoft patches have been installed on Brainlab Kick and Curve Systems. Customers should contact Brainlab technical support for assistance.

- If you are concerned that a Kick or Curve System has been impacted by a Cyber-attack related to this vulnerability, please immediately disconnect the system from your network and contact Brainlab Customer support at https://www.brainlab.com/customer-support/