CVE-2019-0708 ("BLUEKEEP")
REMOTE DESKTOP SERVICES REMOTE CODE EXECUTION VULNERABILITY

On May 14, 2019, Microsoft published a security vulnerability advisory, CVE-2019-0708, related to Remote Desktop Services. We are monitoring updates related to this vulnerability and are evaluating our products that use the affected Microsoft Operating Systems.

Based on our current knowledge, the following Boston Scientific systems may be impacted by this vulnerability:

Boston Scientific System	Uses Remote Desktop Services?
iLAB™ Ultrasound Imaging System	• Yes, Acquisition PC can use Remote Desktop Protocol (RDP) to provide access for performing a software upgrade of the Acquisition PC. • Delivered with Remote Desktop Protocol (RDP) disabled on network-facing (Image) PC. • Externally filtered by optional Network Security Device (NSD) appliance.
POLARIS™ Imaging System	• Yes, Acquisition PC can use Remote Desktop Protocol (RDP) to provide access for performing a software upgrade of the Acquisition PC. • Delivered with Remote Desktop Protocol (RDP) disabled on network-facing (Image) PC. • Externally filtered by optional Network Security Device (NSD) appliance.
FusePanel® endoscopic image system	No - Delivered with Remote Desktop Protocol (RDP) Disabled.
LABSYSTEM PRO™ EP Recording System	No - Delivered with Remote Desktop Protocol (RDP) Disabled.
Clinician Programmer for Neuromodulation Systems with model numbers M365NM7153xxx based on a tablet manufactured by ASUS	No - Delivered with Remote Desktop Protocol (RDP) Disabled.
Rezūm™ water vapor therapy system	No – there is no networking hardware installed in the device.

To date, we have not received any reports of this vulnerability causing issues on our devices.

The Boston Scientific team is dedicated to ensuring the safety and security of our products used every day by patients and clinicians worldwide. As we complete the analysis of each potentially impacted product, we will communicate through our normal customer communications methods:

- Recommended mitigations or,
- If patching is required, the anticipated schedule for that patch.

Revision 2 – July 1, 2019