CVE-2021-34527 (“PrintNightmare”)
Windows Print Spooler Remote Code Execution Vulnerability

The remote code execution (RCE) vulnerability identified in the Microsoft Windows Print Spooler Service known as PrintNightMare or CVE-2021-34527 has low risk of impacting the Boston Scientific LabSystem™ PRO EP Recording System. After an evaluation of devices currently in use, we can confirm that, to date, we have not received any feedback that Boston Scientific LabSystem PRO products have been affected by the PrintNightMare vulnerability.

Vulnerability Detail:

The LabSystem PRO EP Recording System is built on the Microsoft Windows operating system. According to Microsoft, a remote code execution vulnerability exists when the Windows Print Spooler Service improperly performs privileged file operations. An attacker who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs, view, change, delete data, or create new accounts with full user rights.

Affected LabSystem PRO EP Recording System Computer Models:

- LS8900 - LabSystem PRO EP Recording System w/ Windows 7 Operating System (M00420020290)
- LS9900 - LabSystem PRO EP Recording System w/ Windows 7 Operating System (M00420020340)
- LS10K - LabSystem PRO EP Recording System w/ Windows 10 Operating System (M00420020810)

Recommendations:

We strongly caution our customers against modifying the LabSystem PRO EP Recording System. Per the instructions for use (IFU), “The LabSystem PRO EP Recording System is provided complete and ready for use. To ensure appropriate/proper compatibility and interface, the installation or connection of additional hardware, software, or updates of any kind to the LabSystem PRO platform, other than that which is provided by and/or approved by Boston Scientific is prohibited.”

Customers who are concerned about the susceptibility of LabSystem PRO in their EP Lab can employ the following temporary measure to reduce the likelihood of exposure:

1. Disconnect LabSystem PRO from the clinic network. This will disable the connection to the EMR/HIS system, network archive location and network printer.

Mitigation:

For LS8900 w/ Win7 or LS9900 w/ Win7 Operating Systems, BSC will perform the following mitigation (per Microsoft) on the LabSystem Computer upon next service visit or upon request:

- Disable inbound remote printing by setting policy “Allow Print Spooler to accept client connections” to ‘Disabled’.

Note: This mitigation will not affect local printing or printing to a network printer.

For LS10K w/ Win 10 Operating System, BSC will perform the security update on the LabSystem Computer upon next service visit or upon request. This security update contains the appropriate patch KB5004948 (per Microsoft).

Please contact your field service representative with any questions about these precautionary measures or any other concerns regarding our response to this matter.

Revision 2- March 21, 2023