BWI Updated Statement on Microsoft “PrintNightmare” Vulnerability

September 2022

Security of medical devices is of utmost importance to all Johnson & Johnson Medical Device subsidiary companies, and we strive to maintain the best in industry security practices. We constantly monitor for vulnerabilities that could impact the safe operation of our portfolio of software-enabled medical devices, and we partner with each Johnson & Johnson Medical Device subsidiary company to define and execute timely remediation.

Microsoft announced a critical vulnerability affecting versions of Windows with the Print Spool service enabled. This announcement has been formalized in Microsoft’s security update guidance CVE-2021-34527, known as Windows Print Spooler Remote Code Execution Vulnerability.

We have identified the following Johnson & Johnson Medical Device subsidiary company products as running versions of Windows with the vulnerable Print Spool service enabled:

- CARTO® 3 System, running software Versions 6 and Version 7.1.

ACTION REQUIRED:

Biosense Webster has released the Security Service Pack 4 (KT-0001-17/U), which includes the fix for this vulnerability. Please contact your local sale team to order and install this Security Service Pack to address the Print Spooler Vulnerability if you have the CARTO 3 Systems with the versions listed below:

- V6.0.70.100
- V6.0.70.211
- V6.0.80.45
- V6.0.80.122
- V7.1.80.33

Thank You

We appreciate your commitment to Johnson & Johnson as we work on patching to implement best security practices for our devices. If you have additional questions about this letter, please contact us at ProductSecurity@its.jnj.com