Statement on Microsoft "PrintNightmare" Vulnerability

Security of medical devices is incredibly important to all Johnson & Johnson Medical Device subsidiary companies, and we strive to maintain best in industry security practice. We are constantly monitoring 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.

Recently Microsoft announced a critical vulnerability affecting versions of Windows with the Print Spool service enabled. This has been formalized in Microsoft's security update guidance CVE-2021-34527, commonly referred to as PrintNightmare. We have identified the following Johnson & Johnson Medical Device subsidiary company products as running versions of Windows with the vulnerable Print Spool service enabled:

- **Biosense Webster** – CARTO 3 Versions 6 + Version 7
- **NeuWave** – Neuwave Microwave Ablation System and Ablation Confirmation software
- **Johnson & Johnson Surgical Vision**: LipiScan, LipiView and LipiFlow product lines

We are actively working to develop and implement patches or other controls. We will provide additional information regarding a fix or compensating controls at a future date.

Thank You

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