Statement on Blackberry's QNX BadAlloc Vulnerability

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

Recently, Blackberry announced a vulnerability affecting versions of QNX real-time operating system that has a *calloc()* library function. This has been formalized in Blackberry's security update guidance CVE-2021-22156, commonly referred to as badAlloc vulnerability.

We have identified the following J&J products as running versions of QNX with the badAlloc vulnerability:

- **IFS® ADVANCED FEMTOSECOND LASER**
- **COMPACT INTUITIV™ System**
- **SOVEREIGN® COMPACT**
- **WHITESTAR SIGNATURE® PRO System**
- **VERITAS™ Vision System**

We have determined that the risk associated with this vulnerability is controlled with respect to affected J&J products. Nevertheless, we are actively working to identify compensating controls or other mitigations to further remediate this vulnerability as quickly and safely as possible. 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