Boston Scientific
Advancing science for life™

CVE-2020-0601 (ALSO KNOWN AS CURVEBALL) WINDOWS CRYPTOAPI SPOOFING VULNERABILITY

The Boston Scientific team is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the January 14, 2020 announcement regarding the vulnerability in the CryptoAPI in newer Windows-based systems. With this vulnerability, spoofed Elliptic Curve Cryptography (ECC) certificates appear to originate from a valid source.

Our product security team has assessed our medical systems that may use the affected Windows operating system versions – Windows 10, and Windows Server 2016/2019. At this time, we are not aware of any Boston Scientific medical system in the field that is subject to this vulnerability. This includes our patient implanted devices which do not use 3rd party operating systems. If this changes, we will provide an update.

For more detail, refer to:

- Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
- NSA: https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF

February 4, 2020