Boston Scientific
Advancing science for life™

CVE-2020-10713 (ALSO KNOWN AS BOOTHOLE)
GRUB2: CRAFTED GRUB.CFG FILE CAN LEAD TO ARBITRARY CODE EXECUTION DURING BOOT PROCESS

The Boston Scientific team is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the July 29, 2020 announcement regarding a vulnerability identified in the GRUB2 bootloader program used in many versions of the Linux operating system. The researchers at Eclypsium who identified the initial vulnerability also identified methods that could allow Microsoft Windows systems, using a boot option known as Secure Boot, to be affected by this same vulnerability.

There have not been any reported cyberattacks on Boston Scientific products using this vulnerability.

Our product security team has assessed our devices that use Linux or Windows Secure Boot and have determined that the vulnerability risk is low enough, due to the need to gain remote elevated privileges, the patches for this vulnerability can be applied at the next scheduled software update. No urgent patching is required.

If we learn of information that changes this assessment, we will provide an update.

For more detail, refer to:

- Eclypsium: https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

September 16, 2020