OVERVIEW

Abbott Medical Optics Inc. (hereinafter referred to as "J&J Vision") manufactures and sells several products running a variety of operating systems; however, most of them are not directly impacted by the SMBv1 (commonly known as the "WannaCry Ramsomware") vulnerability **due to lack of customer network connectivity.** The list below provides details on operating systems and network connectivity for our surgical products. For the Catalys® Laser Precision System please read the remainder of the bulletin for details on mitigating controls.

- ***iDESIGN*** system 1.x – Windows XP SP 3 – Standalone device **not connected** to the customer network
- ***STAR*** Excimer Laser (S4, S4IR) – Windows 2000 - Standalone device **not connected** to the customer network
- **Whitestar Signature Pro** Phaco System– Windows 7 Embedded – Standalone device **not connected** to the customer network
- **WHITESTAR® Signature System** Phaco System – Windows XP Embedded- Standalone device **not connected** to the Network
- **Compact Intuitiv** Phaco System – QNX, Version 6.5.0- Standalone device **not connected** to the customer network
- **SOVEREIGNTM System** Phaco System – QNX, Version 6.2.1- Standalone device **not connected** to the customer Network
- **SOVEREIGN® Compact System** Phaco System – QNX, Version 6.2.1- Standalone device **not connected** to the Customer Network
- ***iFS*** or ***IntraLase FS*** Femtosecond lasers – QNX, Version 6.3.2/6.5.0 – Connected, but **not running Windows**
- **Catalys® Laser Precision System-** Windows 7 Pro and **connected to the network**

***PLEASE READ REMAINDER OF THE BULLETIN IF YOU USE A CATALYS® LASER SYSTEM*.**

AFFECTED PRODUCT - CATALYS® LASER SYSTEM

J&J Vision has identified mitigated vulnerabilities associated with the Catalys® Laser System regarding the Wannacry ransomware and use of SMBv1. The Catalys® Laser Precision System has existing cybersecurity controls in place preventing infection from the Wannacry ransomware threat for our customers. J&J Vision is in the process of developing a Cybersecurity Update to address the vulnerabilities on the core operating system. The remainder of this document provides an overview of the Impact, and Mitigation relating to the SMBv1 and Catalys® Laser Precision System.

IMPACT: Successful exploitation of these vulnerabilities may allow an attacker to remotely access the device and upload a payload for execution (e.g. Ransomware). Several mitigations (as listed in the Mitigation section below) exist for these vulnerabilities, severely limiting the attack surface.

MITIGATION

J&J Vision is in the process of developing a Cybersecurity Update to address the vulnerabilities listed above. J&J Vision also identified the following existing mitigating controls for customers:

- The Catalys® Laser Precision System is segregated from a customer's network, through an integrated hardware firewall. The hardware firewall blocks all inbound ports and only allows ports 80/443 outbound for remote servicing and printing.
- Networking on the Catalys® Laser Precision System is disabled by default and only enabled under the following circumstances:
    - User is actively printing and networking is enabled for 5-10 minutes.
    - User has pressed the "enable network button" to allow remote service. The network stays enabled until the user presses the "disable network button", when the next treatment starts or upon system reboot.
- If you are concerned a Catalys® Laser Precision System has been impacted by a Cyber-attack, please take the following actions:
    - Remove the network cable to disconnect the system from the network.
    - Contact the J&J Service Department at +1.800.511.0911, Option 4, or Tech_Support@abbott.com.