



Image Stream Medical, Inc.

One Monarch Drive

Littleton, MA 01460

Phone: 978.486.8494

Fax: 978.428.2694

Security Update: WannaCry ransomware

WannaCry ransomware is a fast-propagating cryptoworm which exploits the Microsoft Windows Operating System, allowing the virus to move through a network infecting other systems. The result is loss of data or the need to pay ransom to regain control of the data. The vulnerability was published as Microsoft Security Bulletin MS17-0101 on March 14, 2017 and Microsoft released a security update to address the WannaCry attacks.

On May 12, 2017, the WannaCry ransomware was used in a worldwide cyberattack and in the first day more than 230,000 computers in 150 countries were affected.

Impact of WannaCry on Image Stream Medical products

Image Stream Medical (ISM) products may be temporarily impacted if they are connected to a network and do not have the Microsoft security update applied, but are protected against data loss.

This includes the following devices:

- EasyLink™ Router
- EasySuite® Thin Client PC
- nCare™ RX
- nCare™ MX
- nStream® GX
- LiveStream™ StatusBoard

The MedPresence™ vSuite device, deployed on a hardened Windows 10 platform, is not susceptible to the WannaCry virus.

If infected, an ISM device cannot be used while the virus is in memory. As a matter of good practice, ISM recommends monitoring your network and isolating any devices or systems suspected of being infected by any kind of malware or virus.

ISM Devices built to clear WannaCry

All Image Stream Medical devices are protected from the worst effects of the WannaCry virus. All ISM devices employ a Microsoft embedded operating system feature called File-based Write Filter (FBWF) which protects them from unauthorized changes. For these protected devices, the FBWF redirects any write operations to a RAM cache overlay.

This means that the effects of the WannaCry virus can be cleared from any ISM device by simply rebooting it, all without losing any clinical data.

Once an infected device has been cleared, it should be updated with the recommended Microsoft security patch to prevent future reinfection.

The ISM Response

Image Stream Medical takes the security of its products and information stored on its products very seriously and has taken a proactive approach to address the effects of the WannaCry virus.

ISM immediately responded after the attack, and on May 24, 2017, notified customers of approved Microsoft security updates to address the WannaCry virus on our website:

http://www.imagestreammedical.com/wp-content/uploads/2017/05/Microsoft_Update_Notification_2017_May_24_WannaCry.pdf

Recognizing the severity of this attack, ISM service has proactively installed the Microsoft security update remotely to customer devices or has helped hospital IT departments install the update on server systems.

For systems that have not yet been updated, the WannaCry update can be installed remotely by ISM Support personnel or on site by Field Service personnel. Once the patch is installed, the device has immunity to the WannaCry virus and can no longer be affected, even temporarily.

If a customer is unsure whether the WannaCry patch has been applied to Image Stream devices or servers, please contact Image Stream Technical Support at 866-376-6800.

All new devices shipping from Image Stream Medical have the necessary updates already applied and are fully immune to the WannCry virus.

Note, ISM VaultStream™ enterprise content management systems run on hospital supplied servers. The timing and performance of updates to hospital supplied servers are controlled by the institution's IT department.