**May 19, 2017**

On Friday May 12, 2017, a ransomware computer worm targeting Microsoft Windows operating systems was identified. It is estimated that more than 150 countries, over 200,000 computers have been affected by this attack. The ransomware displays a message on the user's computer informing them that their files have been encrypted, and a payment is required within a certain amount of time in order to decrypt said data. Microsoft has released MS17-010 Security Bulletin to address the vulnerability being exploited by the worm.

The following Olympus products have been tested and validated with the MS17-010 patch:

- Knowledge Exchange (KE)
- IN10A
- EndoCapsule
- Image Stream Medical nStream and VaultStream

**Note:** Olympus no longer publishes approved Windows Updates for EndoWorks. However if a customer's internal security policy permits, customers may attempt to apply the appropriate MS17-010 patches on EndoWorks if they have completed a full system backup prior to patch application. Failed patch attempts requiring on premise software assistance by Olympus may necessitate customer incurred charges.

In all instances, customers electing to deploy the MS17-010 security bulletin based on their facility's security policies should first ensure that there is a valid immediate backup. Customers may contact Olympus' Technical Assistance Center at 800-848-9024 if they require any assistance backing up or restoring their data.

This page will be updated as new information becomes available.

More information and guidance from Microsoft can be found at

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/