Avaya became aware of the “WannaCry” ransomware attack on Friday, May 12, 2017. Avaya teams have assessed the risk related to servers and endpoints, as well as the risk introduced by external connections and partners, contractors, and vendors. At this time, Avaya has not identified any systems that have been impacted by the attack. Our Incident Response Team continues to work closely across internal operational groups to ensure all systems are appropriately patched. Avaya IT had already patched externally-facing systems, completed internal systems, and is pursuing outliers related to server decommission and offline endpoints. These systems are protected by advanced firewall services and anti-virus definitions. We will continue to proactively track activities for the initial attack vector, as well as any expected variants.

As it relates to applicable Avaya products, please ensure you have installed the March Microsoft Patch, MS17-010 Security Update: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. If you have any additional questions related to your Avaya product, please submit a ticket via support.avaya.com.