Hitachi Healthcare Americas Risk Assessment for the Wannacry Ransomware Attack

Twinsburg, Ohio May 25, 2017

Hitachi Healthcare Americas ("Hitachi") has conducted a risk assessment of the Wannacry ransomware attacks and is issuing this cybersecurity advisory to its customers.

On Friday, May 12 hospitals, schools, companies and government organizations were the victims of a cyberattack using the ransomware known as WannaCry (or WannaCrypt). This has impacted organizations and individuals worldwide shutting down an estimated 230,000 computers in at least 150 countries including the United States, United Kingdom, Russia, France and Japan.

Ransomware infects a computer when a user opens a phishing email, triggering a software download that spreads to any vulnerable networked computer. The ransomware locks all the files on the computer and displays the message "Ooops, your important files are encrypted" until the ransom is paid. The Wannacry ransomware uses the ExternalBlue exploit and DoublePulsar backdoor to spread. A critical patch has been issued by Microsoft on March 14 2017 (MS17-010) to remove the underlying vulnerability but many organizations may have not yet deployed this patch. Computer systems running various versions of the Microsoft Windows operating system may be vulnerable if not patched or otherwise protected.

Hitachi takes cybersecurity very seriously and we are in the process of reviewing our product portfolio for potential risks. As of the date of this posting, we have not received any notice from our customers that any of our MR, CT or Ultrasound products were infected by the ransomware. The following is an update on the status of our review.

Magnetic Resonance and Computed Tomography Risk Assessment

Hitachi MRI systems MPR-5000, MRP-7000, Altaire, AIRIS, AIRIS II, and AIRIS Elite do not use the Microsoft Windows operating system and are not vulnerable to the WannaCry ransomware. Additionally, Hitachi MRI and CT systems with a Windows Operating System are equipped from the factory with a hardware firewall that blocks the ports (SMB ports 137,138, 139, 445) that allow the ransomware to infect a system. It is possible that your IT department requested that these ports be unblocked in which case your system may be susceptible to attack. Hitachi strongly recommends that you confirm with your IT department that these ports remain blocked and that they have not changed. We are currently in the process of evaluating our installed base

of MR and CT systems to determine the availability of a patch based on the model of the system you deploy and our strategy for rolling this patch out to our installed base. Should you have any questions as pertains to the status of your particular model, please call the number below.

Ultrasound Risk Assessment

Hitachi ultrasound systems using a Microsoft Windows operating system may be vulnerable to the WannaCry ransomware. If your system is not connected to a network, there is no way for the ransomware to infect the system. We are currently in the process of evaluating our installed base of ultrasound systems to determine the availability of a patch based on the model of system you deploy and our strategy for rolling this patch out to our installed base. Should you have any questions as pertains to the status of your particular model, please call the number below.

Customers that require further information should contact Hitachi Healthcare customer service at **1-800-800-4925**. Your call will be routed to a member of our cybersecurity team, who will ensure your inquiry will be most efficiently processed.

Sources:

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

http://www.cio.com/article/3196792/antivirus-software/how-a-22-year-old-accidentally-flipped-the-wannacry-kill-switch.html