Date: May 24, 2017 at 2:38:08 PM EDT
To: <NHISAC-AMBER@LISTSERV.NHISAC.ORG>
Subject: Medical Devices Protected from WannaCry with a Firewall - Sharing of an approach that might be useful
Reply-To: NH-ISAC Amber <NHISAC-AMBER@LISTSERV.NHISAC.ORG>

***TLP WHITE**: Disclosure is not limited. Sources may use **TLP WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP WHITE** information may be distributed without restriction.*

Medical Devices Protected from WannaCry with a Firewall - Sharing of an approach that might be useful

A hardware firewall that isolates the medical device network functions from the WannaCry ransomware infection is an alternative to applying the recommended operating system patch. If a medical device is a closed system (e.g. cannot be used for email or browsing the web) and has been segregated from the Healthcare Delivery Organization (HDO) network through the use of a hardware firewall configured to block the ports used by the WannaCry ransomware, then the operating system patch is not necessary because the firewall protects the medical device from infection.

A firewall deployed with the medical device by the device manufacturer should not be modified and the configuration should remain as specified by the device manufacture to ensure critical or essential communications functions of the device will not be blocked. An HDO installing a firewall to segregate a device should check with the manufacturer or the device manual to verify critical or essential communications functions of the device will not be blocked.

Questions and Answers

Q: The report says to install the Windows patch and then in the same paragraph says you don't need to install the Windows patch if you have a firewall. I would hesitate recommending people not to patch even if they have a properly configured firewall.
A: The intent was in situations where it is not practical to immediately apply the patch, that the firewall can protect from infection. For example, with some medical devices a customer does not have access to the O/S and cannot apply the patch. Ultimately the manufacturer must implement the patch in accordance with their formal release procedures, and will rely on the secure configuration of the firewall to provide protection until that time. Revised and consolidated the wording to clarify the intent.
Q: Blocking port 445 for SMB v1 will only stop the worm from propagating across the network but single workstations potentially could still be infected via usb or phishing email. I would not want to provide a false sense of security by suggesting that if you block the port you don't need to take other defensive measures.
A: The statement of the medical device being a "closed system" was intended to narrow the applicable devices to those that cannot be used for browsing, reviewing email, etc. Additional clarification was added about a closed system.
Q: Do any medical devices depend on SMB v1 to function properly? There have been several medical devices affected by Wannacry that do not function if SMB v1 is blocked. I would add a caveat to the statement regarding blocking SMBv1 ports, if there would be a functional impact to certain products.
A: Consideration of this was given by the statement that if an HDO installs the firewall, then they need to review any settings with the manufacturer. Minor changes were made to clarify manufacturer deployment from HDO installation.

NH-ISAC
NATIONAL HEALTH - ISAC

Thank you.