WannaCrypt malware and Codonics products

Codonics is aware of and has been monitoring the situation with the WannaCrypt ransomware attack that is affecting healthcare facilities globally. To help our customers better understand any possible risk, we've listed Codonics products and their vulnerability to the WannaCrypt/WannaCry malware in the following table:

Product	***Vulnerability Comments***
EP / NP Series Imager	• ***Not applicable (non-Windows based)***
Horizon Imager	• ***Not applicable (non-Windows based)***
Virtua CD/DVD Publisher	• ***Requires software version 4.1.0 or later*** • Follow Codonics instructions (below) for applying patches to the Windows Embedded OS • Alternatively, the malware can be blocked via the built-in firewall. See Windows Firewall instructions below. • New software releases (5.1.0 and later) will include patches
Integrity	• ***Requires software version 1.6.2 or later*** • Follow Codonics instructions (below) for applying patches to Windows Embedded OS • Alternatively, the malware can be blocked via the built-in firewall. See Windows Firewall instructions below.
Infinity / RDSS	• ***Requires software version 1.1.0+ or 1.4.0+*** • Follow Codonics instructions (below) for applying patches to the Windows Embedded OS
Safe Label System (SLS) 500i	• ***Not applicable (non-Windows based)***
SLS Administration Tool (AT)	• ***Configure built-in AT database backup and store on a secured remote device*** • Patch host computer system per Microsoft instructions (link below)
Container Labeling System (CLS)	• ***Backup database and store on a secured remote device*** • Patch host computer system per Microsoft instructions (link below)
Codonics Disinfection Technology (CDT) D6000 and D7000	• ***Not applicable (non-Windows based and non-Network based)***
Codonics Disinfection Technology (CDT) Radius 3	• ***Not applicable (non-Windows based and non-Network based)***

For the SLS AT and CLS, please consult the following link to patch host PCs:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Virtua Software versions 4.1.0 through 5.0.0

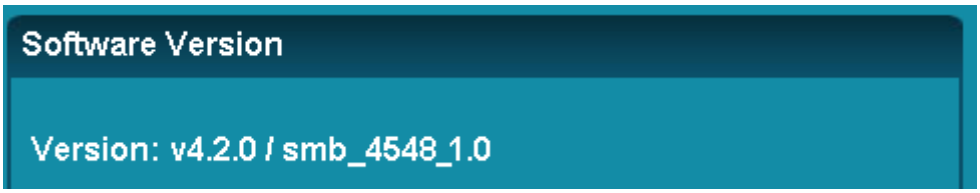
Download the Codonics security update for both Win XP and Win 8 operating systems from:

http://www.codonics.com/Support/Virtua/smb_4548-1.0.exe

Follow the instructions in the Virtua Software Updates Technical Brief to apply the update:

http://www.codonics.com/Support/Virtua/pdf/tech/Software_Updates-901-215-001.pdf

Once the update process is complete, navigate to the Help tab of the User Interface. The version will now have the text string “smb_4548_1.0” appended to it.



Example: Software version v4.2.0 with security patch applied.

Integrity 1.6.2+ (Windows XP Embedded)

Download the English language security update for Windows XP SP3 x86
(not the installer for Windows XP Embedded SP3 x86) from:

http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe

Follow the instructions below to apply the updates:

1. Transfer the update file to the system's SmartDrive (by either copying over the network or physically removing).
2. Attach a mouse and keyboard to the USB ports.
3. Press the Windows Key + D on the keyboard to hide the Codonics user interface.
4. Press the Windows Key + E on the keyboard to open a Windows Explorer window.
5. Left-click the SmartDrive (labelled CODONICS).
6. Press Enter on the keyboard to navigate to that drive (double-click is disabled).
7. Left-click the update file on the SmartDrive.
8. Press Enter on the keyboard to run the file (double-click is disabled).
9. Click the Next button.
10. Click the I Agree checkbox, and click the Next button.
11. Wait for the update to install.
12. Click the "Do not restart now" checkbox, and click the Finish button.
13. Press and hold the Alt button the keyboard.
14. While holding the Alt button, press the Tab button until the Firefox window is selected, then release both buttons. This will display the Codonics user interface.
15. Manually reboot the system from the Codonics user interface.

Windows Firewall for Virtua / Integrity

If you are not using any file-sharing features, you may block the network port used to spread the malware.

1. Set the following fields in the Network Profile contained on the SmartDrive:

firewallEnabled_ = true
smbFileShareFirewallPortOpen_ = false

2. Manually reboot the system from the Codonics user interface.

NOTE: Setting these fields will disable file sharing, which includes the Direct-to-Disc feature on Virtua, and Remote SmartDrive Access on both products.

RDSS 1.1.0+ / Infinity 1.4.0+ (Windows XP Embedded)

Download the Windows XP SP3 update from:

http://www.download.windowsupdate.com/msdownload/update/software/dflt/2008/04/windowsxp-kb936929-sp3-x86-enu_c81472f7eeea2eca421e116cd4c03e2300ebfde4.exe

Download the English language security update for Windows XP SP3 x86
(not the installer for Windows XP Embedded SP3 x86) from:

http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe

Follow the instructions below to apply the updates:

1. Copy the downloaded patches above to a USB flash drive.
2. Log in as “admin” on the Infinity.
3. At the desktop, click the Start Menu, then My Computer.
4. Identify the drive letter of the USB flash drive, and double-click to open it.
5. Double-click the SP3 update file (windowsxp-kb936929-sp3-x86-enu_c81472f7eeea2eca421e116cd4c03e2300ebfde4.exe).
6. Follow the onscreen instructions and reboot when prompted by clicking Finish.
7. Log in as “admin” once the reboot has completed.
8. At the desktop, click the Start Menu, then My Computer, then double-click the USB Flash Drive again.
9. Double-click the security update file (windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe).
10. Wait for the update to install.
11. Click the "Do not restart now" checkbox, and click the Finish button.
12. Click the Start Menu, then My Computer.
13. Right click the USB flash drive, and click “Eject”.
14. Remove the USB flash drive.
15. Click the Start Menu, then Shutdown.
16. Select Restart from the list, and click OK.