May 21, 2017

Dear Customer:

You may have seen the recent news about the WannaCryptor “ransomware” attacks that have spread around the world since late last week. We would like to provide some information about our response to this threat, as well as some information about how to protect yourself.

**What is WannaCryptor?**
WannaCryptor, also known as “WannaCry,” is a type of “ransomware,”a malicious software that uses encryption to effectively lock your files. The only way to unlock your files is to pay a ransom. WannaCryptor is particularly dangerous because it’s also a type of “worm,” meaning that it can spread itself over computer networks without any user interactionby exploiting a security vulnerability in the Microsoft Windows operating system. The good news is that Microsoft released a patch for this vulnerability in March of 2017. Systems that automatically download and apply updates from Microsoft should not be vulnerable to this attack.

**How can you protect your Harmonic products from WannaCry?**

- ProMedia Live Package Origin 1.x: Disable the SMBv1 service through the registry. Contact the Harmonic Technical Assistance Center for assistance.

- All other Windows-based Harmonic products: Ensure that you have patched all your computers that run Windows. More information can be found here:

  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

The patches can be downloaded from the following locations:

Windows Server 2003 SP2 x64
(http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe)

Windows Server 2003 SP2 x86
(http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-enu_f617caf6e7ee6f43abe4b386cb1d26b3318693cf.exe)

Windows XP SP2 x64
(http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe)

Windows XP SP3 x86
(http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe)

Windows XP Embedded SP3 x86
(http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-enu_8f2c266f83a7e1b100ddb9acd4a6a3ab5ecd4059.exe)

Windows 8 x86,
(http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu)

Windows 8 x64
(http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu)

Windows Server 2008 R2 for x64-based Systems Service Pack 1
(http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu)

Windows Server 2012 R2
(http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu)

You should also block outbound “SMB” traffic at your firewalls so that you don’t spread the malicious software to other computer networks across the Internet.

If your system is infected, you may notice files with new extensions (e.g., “.wnry”, “.wcry”, “.wncry” or “.wncryt”), or a pop-up window may appear asking you to pay a ransom. If you suspect that your system is infected, turn it off immediately to stop the loss of data. Contact your IT or Security team and follow their instructions.

Best regards,

Harmonic Service & Support