Product Notice #0314

Protecting Windows Server-based AudioCodes Products from WannaCrypt Malware

Dear Partners and Customers,

This Product Notice announces a Windows security update for the WannaCrypt malware.

WannaCrypt is a ransomware program targeting Microsoft Windows servers and computers. In May 2017, a large cyber-attack was launched using WannaCrypt.

Although Microsoft released a security update that protects against this attack, systems based on Windows that were not updated with this security update are vulnerable to this attack and may have been affected. For more information, see https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/ and https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

The following AudioCodes products use windows operating system and as such, may be vulnerable to this malware:

- Mediant Survivable Branch Appliance
- CloudBond 365™
- Mediant CCE Appliance for Microsoft Cloud PBX
- Auto Attendant IVR and Fax Server
- SIP Phone Support (SPS)
- Voice Mail Server
- VocaNOM

Corrective Action

Customers whose servers were updated with Windows server security updates should be protected from this vulnerability. However, we **highly recommend** that you verify that your system has indeed been installed with the latest updates. To check that your system is updated with latest security update, connect to your system using Remote Desktop Connection, open Windows Installed Updates and verify that your system includes Security Update for Microsoft Windows" from April 2017 or later.

Customers whose servers are not installed with Windows server latest updates **must** install the latest Microsoft security updates, available from the Microsoft download center and according to your AudioCodes product:

1. Download the latest Microsoft Security Update file from the links below.
2. Connect to the AudioCodes server using Remote Desktop Connection, and then copy the downloaded file to a temp directory.
3. From the temp directory, run the Microsoft security update and follow its instructions:

- **Mediant SBA for Microsoft Lync 2010/2013 (Windows Server 2008R2):** https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264
- **Mediant SBA for Microsoft Skype for Business (Windows Server 2012R2):** https://support.microsoft.com/en-us/help/4019215/windows-8-update-kb4019215
- **CloudBond 365 (Windows Server 2012R2):** https://support.microsoft.com/en-us/help/4019215/windows-8-update-kb4019215

  Note: You need to run this update on all CloudBond 365 virtual machines (i.e. Edge, FE, DC, Reverse Proxy) and the Host server. To install the update for each virtual machine, connect to it either through Remote Desktop Connection or using the Hyper-V Manager tool from the Host server.

- **Mediant CCE Appliance for Microsoft Cloud PBX (Windows Server 2012R2):** https://support.microsoft.com/en-us/help/4019215/windows-8-update-kb4019215

  Note: You need to run this update on all CCE Appliances virtual machines (i.e. Edge, Mediation server, DC, CMS) and the Host server. To install the update for each virtual machine, connect to it either through Remote Desktop Connection or using the Hyper-V Manager tool from the Host server.

  For the CCE Appliance, you also need to replace the Windows VHDX image on the CCE Appliance host:

  a. Download the new Windows VHDX image from: http://downloads-audiocodes.s3.amazonaws.com/CCE%20V1/SFBServer.zip
  b. On the host server, open PowerShell and then run **Get-CcSiteDirectory** to return the current bits root directory.
  c. Copy the downloaded SFBServer.zip file to <bits root directory>\Bits\VHD (you can back up the old zip file).
  d. Delete the SFBServer.vhdx file from this directory and unzip the downloaded SFBServer.zip file.

  To update the CCE Appliance's USB recovery dongle, copy the downloaded SFBServer.zip file to <USB root>\CCESources\Bits\VHD.

- **SIP Phone Support – SPS (Windows Server 2008R2):** https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264
- **Voice Mail Server (Windows Server 2012R2):** https://support.microsoft.com/en-us/help/4019215/windows-8-update-kb4019215
- **Auto Attendant IVR and Fax Server (Windows Server 2008R2):** https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264

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

  For more information, see https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

- **VocaNOM:**

  - **Windows Server 2008R2:** https://support.microsoft.com/en-us/help/4019264/windows-7-update-kb4019264
  - **Windows Server 2003:** http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe

  For more information, see https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

Note:

- After you install the Microsoft update, you may have to restart your system (according to the Windows update instructions).
- To protect your system in the future, it is important that you periodically update your Windows system with the latest Microsoft security updates.
- In the next AudioCodes software release, AudioCodes products will be shipped with this security update. Until then, customers should update the Windows system **as soon as possible** with the Microsoft security update per instructions in this Product Notice.
- For Windows systems that have already been affected by this security vulnerability, you need to re-install (recover) your system and then immediately install it with the latest Windows security updates. For more information on product recovery, please refer to the product's *User Manual*.
- For customers (CloudBond 365, Auto Attendant IVR, Fax Server, Voice Mail Server, and VocaNOM only) that periodically back up their system, use the most recent backup.