PHILIPS

****** URGENT FIELD SAFETY NOTICE ******

Re: **Philips Volcano s5i, CORE, and CORE Mobile systems with software version v3.5**

November 21st, 2017

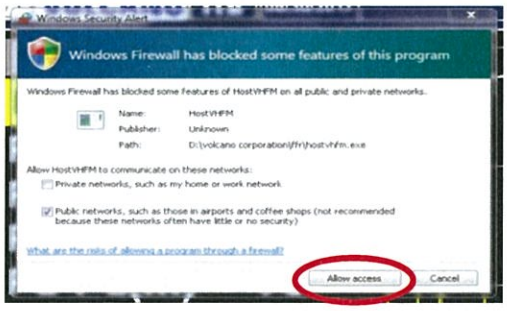
Dear Cath Lab Manager:

If you have a device that meets the criteria below – your system may be impacted:

Product Part Number	Product Description	Manufacturing Date and SW version
807400001	Volcano Imaging System s5i	March 23, 2016 – October 18, 2017 version v3.5 software
400-0100.01, 400-0100.01-R 400-0100.07 400-0100.07-R 400-0100.08 400-0100.08-R	CORE Mobile Imaging System (120V) CORE Mobile Imaging System Refurbished CORE Mobile Imaging System (240V) CORE Mobile Imaging System Refurbished CORE Mobile Imaging System (100V) CORE Mobile Imaging System Refurbished	
400-0100.02	CORE Imaging System	

You are receiving this letter because our records indicate you have a potentially Impacted System.

The Microsoft Windows security settings on a small number of Impacted Systems were incorrectly configured during the manufacturing process. This misconfiguration can lead to a Windows Security Alert dialog being displayed when the system is switched from IVUS to the FFR/iFR mode. If the user responds to the dialog by selecting "Allow Access," (as shown below), the device's network firewall settings will be modified, opening its network ports to potential unexpected communication from the hospital network to which the device may be connected.



Unexpected communication from the hospital network could include normal network security operations, e.g., port scanning. If these communications occur during an active FFR/iFR procedure, data recording could be affected leading to:

- Incorrect FFR/iFR measurements
- Case delay during troubleshooting and/or port scanning
- Abandonment of use of the system

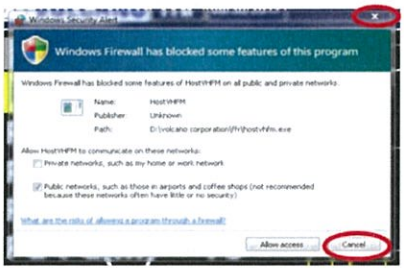
Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95640 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

PHILIPS

Based on our investigation there is only a remote probability that any of these impacts may occur.Philips Volcano Service will perform an inspection of the system configuration as part of the Preventive Maintenance or Service process and will correct the configuration if necessary. This will occur within the next 12 months. Until that time, you may continue to use your system provided that you take the following steps:

1. If possible, before starting a patient case, reboot the system and once the system has completed the startup sequence, switch to FFR/iFR modality. If the Windows Alert Dialog appears, select "Cancel" or the "X" in the top right corner. (See image below)



2. If you are in performing a procedure you also may choose to disconnect the Impacted System from the hospital network.

3. If the Windows Security Alert appears on an Impacted System, contact the Philips Volcano Technical Support team to schedule a service visit to correct this condition

Any changes to the firewall permissions made by selecting "Allow Access" will be automatically removed when the system is restarted. However, the Windows Security Alert may reappear after each successive reboot or startup.

Please ensure that a copy of this letter is provided to all personnel within your organization who handle these products. Please complete, sign, and return the attached form indicating that you received this Field Action notification.

Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95670 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO

PHILIPS

We recognize the inconvenience this may cause you, your staff, and your patients. However, this action reflects Philips' commitment to patient safety and high quality standards.

Thank you for your prompt attention to this important matter. On behalf of Philips, we appreciate your partnership and your continued support.

Sincerely,

Peter Dekempeneer
QA & RA Manager International

Philips Volcano
Philips Volcano, 2870 Kilgore Road, Rancho Cordova, CA 95670 USA
www.volcanocorp.com, Tel 800 228 4728, Fax 916 638 8812

VOLCANO