3080 Yonge Street, Suite 6100, Box 66
Toronto, ON M4N 3N1 Canada
T +1.416.484.5000
F +1.416.484.5001
TF +1.866.416.4636
visualsonics.com

CYBERSECURITY ALERT

Dear VisualSonics customer,

FUJIFILM VisualSonics, Inc. ("VSI") is aware of the CVE-2020-16898 (a.k.a "Bad Neighbor" or “Ping Of Death“) vulnerability in Windows 10, and we have evaluated the potential impact of this issue on our imaging systems. Microsoft, the manufacturer of Windows 10, has communicated that the TCP/IP stack in Windows 10 is vulnerable through this exploit. VSI can confirm that the following currently supported pre-clinical imaging systems are not affected by this vulnerability:

Vevo 2100 Vevo LAZR Vevo 1100
Vevo 3100* Vevo LAZR-X* Vevo 3100LT*

* The Vevo 3100, LAZR-X, and 3100LT platforms were switched to Windows 10 starting in early March 2020. Any of these 3 system models which were purchased and installed before that time are not vulnerable. Newer systems, or those older systems which have been upgraded to Windows 10, are affected. Additionally, the recently released Vevo F2 platform runs Windows 10 and thus is also vulnerable.

To date, there are no known implementations of this vulnerability that can be used to execute custom code against a targeted system.

VSI is committed to ensuring that its products are safe, secure, and reliable. We are currently evaluating and testing Microsoft security patches for this exploit. When this process is completed, we will release patches, or updated system software, for the following products:

Vevo 3100 Vevo LAZR-X
Vevo 3100LT Vevo F2

VSI will notify customers when patches, or updated versions of system software, are released. Should you have any questions in the interim, please contact VSI technical support:

website:	www.visualsonics.com/support
email:	support@visualsonics.com
phone:	NA: 1 866.416.4636 EU: +800.0751.2020 ROW: +1 416.484.5000