

CYBERSECURITY ALERT

Dear VisualSonics customer,

FUJIFILM VisualSonics, Inc. ("VSI") is aware of vulnerabilities CVE-2021-24074, CVE-2021-24094, and CVE-2021-24086 in the Windows 7, 8.1, and 10 operating systems. We have evaluated the potential impact of these issues on our imaging systems.

Microsoft, the manufacturer of Windows, has communicated that the TCP/IP stack in these 3 versions of Windows is vulnerable through these exploits. VSI can confirm that the following currently supported pre-clinical imaging systems are affected:

Vevo 1100	Vevo 2100	Vevo LAZR	Vevo F2
Vevo 3100	Vevo LAZR-X	Vevo 3100LT	

To date, there are no known implementations of these vulnerabilities that can be used to execute custom code against a targeted system, and the exploits themselves are considered theoretical.

VSI is committed to ensuring that our products are safe, secure, and reliable. We are currently evaluating and testing Microsoft security patches for these vulnerabilities. When this process is completed, we will, where possible, release patches or updated system software for all of the affected imaging systems.

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