**May 22, 2019**

**Product Security Update - Microsoft Remote Desktop Protocol Vulnerability**

**CVE-2019-0708 Remote Desktop Protocol Vulnerability (Bluekeep)**

As part of our Product Security program, Accuray Incorporated is monitoring the Microsoft security advisory for CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability" and is assessing the associated potential risks. This vulnerability affects systems that use Remote Desktop Services for Windows XP, Windows 7, Windows Server 2003, and Windows Server 2008. For a more detailed description of this vulnerability, please view the information provided by Microsoft. (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708)

To date, we have not received any reports of this vulnerability impacting clinical use or causing breaches to data security related to our treatment delivery, planning, and database systems: the CyberKnife®, Radixact® and TomoTherapy® Systems, the Accuray Precision® Treatment Planning System, and the iDMS® Data Management System. Accuray continues to monitor the available information regarding this issue and assess for any potential impact on its products.

Accuray is committed to providing you with innovative technology that enables you to confidently deliver the best possible care to your patients. To that end, we employ a multi-modal approach to ensure our products meet strict standards for security and the highest standards in patient care and ease-of-use. Accuray recommends that prudent security practices be employed to minimize the risk potential, including:

- Ensure that components of the Accuray systems are behind the system firewall
- Ensure that only secure/sanitized USB storage devices are utilized
- Ensure your data has been backed up and stored according to your institution policy
- Ensure your disaster recovery procedures are in place

We will update this communication as new information becomes available. All product, product procedure, or site-specific questions should be directed to your Accuray service representative.

If you observe symptoms of malicious activity, please contact your IT team and take proper corrective action, which may include disconnecting your system from the network. After contacting your IT team, you may also contact your Accuray Representative and/or Accuray Service Support (http://www.accuray.com/service/service-support)


1310 Chesapeake Terrace, Sunnyvale, CA 94089 Tel: 408.716.4600 Fax: 408.716.4601 www.accuray.com