August 15, 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 has assessed Accuray products for potential risk against the Microsoft security advisory for CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability". 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)

Affected Accuray systems include

- Radixact® System version 1.x
- CyberKnife® System version 5.x, 7.x, 8.x, 9.x, 10.x and 11.x
- Accuray Precision® Treatment Planning System/iDMS® Data Management System versions 1.x, 2.x
- TomoTherapy® Treatment Delivery System with iDMS System version 1.x
- TomoTherapy H™ Series versions 4.x, 5.x

Accuray service personnel will apply the following mitigations upon customer request:

- Disable Remote Desktop Protocol (RDP) or ensure Network Level Authentication (NLA) is enabled if RDP is enabled
- Close firewall port 3389 (varies with version and configuration)
- For machines that are outside the Accuray firewall, include them within Accuray firewall. To retain the machines outside the Accuray firewall, customer's IT personnel should apply the above rules to the customer's firewall as necessary.

Patch media will be validated and released for affected forward production systems as part of future upgrades.

For CyberKnife system versions prior to 11.x and TomoTherapy H-Series 4.x and 5.1.x systems, it's recommended to upgrade these systems to the latest version of Accuray Precision/iDMS integrated software platform, version 3.x.

Accuray is committed to providing you with innovative technology that enables you to confidently and securely deliver the best possible care to your patients. Please contact your Accuray Service Representative for all product, product procedure, or site-specific questions.

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