ACCURAY

July, 7, 2021

Product Security Update

Kaseya VSA Supply-chain Ransomware Attack

Kaseya Ltd. has published detailed updates about the recent security incident against their remote monitoring and management product, VSA. Information can be found on Kaseya's official website (https://www.kaseya.com/potential-attack-on-kaseya-vsa/).

Accuray does not make use of Kaseya VSA software in its product portfolio or in its corporate infrastructure, and therefore is not identifying any potential security risks from this issue.

Accuray is committed to providing you with innovative technology that enables you to confidently deliver the best possible care to your patients. 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

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).