



**March 8, 2021**

## **Product Security Update – Zerologon Vulnerability**

### **CVE-2020-1472 Netlogon Elevation of Privilege Vulnerability (Zerologon)**

As part of our product security program, Accuray Incorporated has assessed Accuray products for potential risk against the Microsoft security advisory for CVE-2020-1472 "Netlogon Elevation of Privilege Vulnerability". For a detailed description of this vulnerability, please view the information provided by Microsoft. (<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472>)

#### Impact:

Products sold by Accuray impacted by this vulnerability include iDMS® Data Management System versions 2.0.x, 3.0, 3.1 and 3.2.

Patch media has been validated and released for affected products and is being rolled out to customers by Accuray Service.

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>).