March 4, 2022

Customer Security Notice

Axeda Vulnerabilities (https://www.ptc.com/en/documents/security/coordinated-vulnerability-disclosure/axeda-public-advisory)

Issue Summary

As an element of its ongoing Cybersecurity vigilance program, Accuray Incorporated (Accuray) is a member of various industry associations and wire services. Through these channels, Accuray learned of certain vulnerabilities in the Axeda software platform. Axeda is a software tool used for remote service monitoring and diagnostics. Accuray has determined that the recently discovered vulnerabilities in the Axeda software platform affect Accuray products.

While no exploitation of Accuray products has been reported as of the date of this notice, Accuray is issuing this notice to inform affected customers of such vulnerabilities and planned mitigations. It is important to note that Accuray is following controlled vulnerability disclosure protocols coordinated through critical infrastructure protection agencies in several jurisdictions.

Affected Products

This issue affects all Accuray products containing Axeda software, including all TomoTherapy® , Radixact®, CyberKnife®, iDMS® and Accuray Precision® Systems.

Reason for Security Notice

No actual exploitation of this vulnerability on Accuray products has been reported as of the date of this notice. This notice, is to inform customers with affected products about the Axeda vulnerabilities and Accuray's current assessment and plans for mitigations. The Axeda vulnerabilities may lead to, among other things, data breach exposing stored system data and confidential patient information.

The Axeda vulnerabilities do not lead to un-commanded energy outputs or automated motion.

Interim Instructions

Accuray is committed to providing innovative technology that enables you to confidently deliver the best possible care to your patients. Customers may continue to use their Accuray products. Accuray recommends that prudent security practices be employed to minimize the risk potential, including:

- Ensuring that components of the Accuray systems are behind the system firewall

- Ensure that a set of firewall rules or access control list is configured and monitored to allow inbound and outbound traffic only as required for the product
- Ensuring that only secure/sanitized USB storage devices are utilized
- Ensuring your data has been backed up and stored according to your Institution's policy
- Ensuring your disaster recovery procedures are in place

Product Correction

Accuray is incorporating and testing the latest version of the remote access agent where PTC, the maker of Axeda, indicated will resolve these vulnerabilities. Accuray will deploy this new version following completion of testing, and an Accuray Field Service Engineer will contact you to schedule this upgrade.

Contact Information

For questions about this Customer Security Notice, please contact Accuray Customer Support by phone or email, using the Service Request form available at http://www.accuray.com/service-requests.

Sincerely,

GS Jha
CIO & Chief Information Security Officer
Accuray Incorporated
1310 Chesapeake Terrace
Sunnyvale, CA 94089