Olympus Response to SweynTooth Vulnerabilities (ICS-ALERT-20-063-01))

Original Release Date: June 17, 2020 | Last Revised Date: June 17, 2020

Note: This communication is the result of initial and ongoing analysis and represents all actions taken by Olympus as of the last revised date. As a result, the content may change as information of the vulnerabilities are released, or additional actions are completed.

Olympus is aware of and currently monitoring ongoing developments related to the recent public reports of multiple Bluetooth Low Energy (BLE) vulnerabilities collectively known as SweynTooth. These vulnerabilities can affect IoT devices which utilize the BLE wireless communication technology.

Full information on the vulnerabilities can be found at the following United States Cybersecurity and Infrastructure Security Agency (CISA) link:

https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01

Olympus Actions & Mitigation Plan

Olympus consistently strives to enhance the security of our products. As such, a global team has been coordinated and has investigated which Olympus products may be affected by these vulnerabilities.

At this time, no medical product developed by Olympus have been found vulnerable to any of the known SweynTooth vulnerabilities.

This page will be updated as new information becomes available.