Olympus Response to Ripple20/Treck Vulnerabilities (ICS-ALERT-20-168-01)

Original Release Date: July 29, 2020 | Last Revised Date: July 29, 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 various vulnerabilities that affect the Treck TCP/IP stack, collectively known as Ripple20. Successful exploitation of these vulnerabilities may allow remote code execution or exposure of sensitive information.

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

https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

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 Ripple20 vulnerabilities.

This page will be updated as new information becomes available.