Olympus Response to Wind River VxWorks Vulnerabilities (ICSA-19-211-01)

Original Release Date: August 14, 2019 | Last Revised Date: August 14, 2019

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 Wind River VxWorks critical vulnerabilities notification which could allow remote code execution.

Full information and guidance from the United States Computer Emergency Readiness Team (US-CERT), as sponsored by the United States Department of Homeland Security (DHS), can be found at the following link: https://www.us-cert.gov/ics/advisories/icsa-19-211-01

Olympus Actions & Mitigation Plan

Olympus consistently strives to enhance the security of our products. As such, a global team has been coordinated and is currently investigating which Olympus products may be affected by these vulnerabilities. Additionally, for any products that may be affected, Olympus will work to test the patches supplied by Wind River and release once validated.

The following products have been identified as running versions of the vulnerable Wind River VxWorks operating systems:

ESG-150
ESG-200
ESG-300
ESG-400
APU-300

An analysis of each product has concluded that as the vulnerabilities are related to the TCP/IP connection, and with network connections not being available in any of the devices, the vulnerabilities are not exploitable, and therefore the products are not vulnerable. As such, no updates are required at this time.

This page will be updated as new information becomes available.