Olympus Response to URGENT/11 (ICSMA-19-274-01)

Original Release Date: October 16, 2019 | Last Revised Date: October 16, 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 notifications of critical vulnerabilities which could allow remote code execution. Specifically, the vulnerabilities, known as "URGENT/11" exist in IPnet, a third-party software component that supports network communications between computers, and found in the versions of the following operating systems:

- VxWorks (by Wind River)
- Operating System Embedded – OSE (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)

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/icsma-19-274-01.

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. Additionally, for any products that may be affected, Olympus will work to test the patches supplied by Wind River and release once validated, if applicable.

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 as TCP/IP connections are not available in any of the devices, the vulnerabilities are not exploitable, and the products are not vulnerable. As such, no updates are required at this time.

Additionally, it has been determined that no products are affected by the URGENT/11 vulnerabilities in the following operating systems:

- Operating System Embedded – OSE (by ENEA)
- INTEGRITY (by Green Hills)
- ThreadX (by Microsoft)
- ITRON (by TRON Forum)
- ZebOS (by IP Infusion)

This page will be updated as new information becomes available.