Olympus Response to Spectre & Meltdown Vulnerabilities

Original Release Date: January 16, 2018 | Last Revised Date: January 16, 2018

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.

Background

On January 3rd, 2018 two vulnerabilities named Spectre and Meltdown were publicly disclosed. These vulnerabilities exploit CPU architectural design flaws, with Intel, AMD and ARM chips. Spectre breaks the isolation between different applications, allowing an attacker to trigger the speculative execution process and potentially read sensitive data produced. Meltdown breaks a fundamental isolation between user applications and the operating system, allowing attackers to potentially access sensitive information.

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 the Spectre and Meltdown vulnerabilities. Additionally, for any products that may be affected, Olympus will work to validate the patches supplied by the associated vendor.

This page will be updated as new information becomes available.

More 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 in Vulnerability Note VU#584653, found at the link below.

https://www.kb.cert.org/vulns/id/584653