Olympus Response to Spectre & Meltdown Vulnerabilities

Original Release Date: January 16, 2018 | Last Revised Date: March 23, 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. The following lists the products confirmed vulnerable to Spectre and Meltdown as well as the products confirmed not to be vulnerable Spectre and Meltdown.

This page will be updated as new information becomes available.

Products Confirmed Vulnerable to Spectre & Meltdown

Product	Validated and Approved Remediation Steps
Brainlab Kick	Apply the Microsoft Update patch that contains the fix for this system
EasyLink Router v 8.0.5	Please upgrade to EasyLink Router v 8.1
EasyLink Router v 8.1	Apply the Microsoft Update patch that contains the fix for this system
LSSB v 8.0.5	Apply the Microsoft Update patch that contains the fix for this system
LSSB v 8.1	Apply the Microsoft Update patch that contains the fix for this system
MedPresence v 9.0.3.1	Apply the Microsoft Update patch that contains the fix for this system
nCare RX v 8.0.5	Apply the Microsoft Update patch that contains the fix for this system
nCare RX v 8.1	Apply the Microsoft Update patch that contains the fix for this system
nStream GX v 9.0.10	Apply the Microsoft Update patch that contains the fix for this system

Products Confirmed Not Vulnerable Spectre & Meltdown

Product
ProSound F75
ShockPulse SE

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/vuls/id/584653