Update on Impact Investigation Regarding PHP2Shell

Olympus has performed a product impact assessment related to the recently disclosed PHP2Shell vulnerabilities, CVE-2026-109618 and CVE-2026-109619. Based on this assessment to date, Olympus has identified certain older versions of the VaultStream™ product family as affected by these vulnerabilities. Olympus's assessment has not identified any other Olympus product families as being affected at this time.

While these vulnerabilities have been reported as exploited in other environments, Olympus is not aware of any exploitation of these vulnerabilities involving the VaultStream™ Server Software at this time.

Customers using the VaultStream™ Server Software should review the version-specific information provided **here** for information regarding the affected version and recommended remediation measures.

Olympus will continue to monitor developments related to these vulnerabilities and will update this advisory if additional relevant information becomes available. Customers with questions or requiring assistance implementing the recommended remediation measures should contact their Olympus representative or Regional Customer Support Center.

Initial Communication: October 27, 2026

Last Updated: November 5, 2026

This document contains confidential and proprietary information of Olympus. The contents shall not be disclosed, reproduced, duplicated, disseminated, or used for purposes other than authorized in writing by Olympus.