Date:	May 2026
Subject:	**Olympus Security Advisory**
Product:	VaultStream™ Server Software
Model:	Version 10.x and older
Attention:	CISO, CIO, IT Administrator

Dear Customers,

Olympus is committed to continuously improving the security of our products and supporting customers in maintaining the integrity of their network environments. Medical device manufacturers and health care delivery organizations alike have a shared responsibility to work collaboratively to maintain robust cybersecurity protections.

As part of our ongoing process for monitoring vulnerabilities and evaluating their potential impact on both newly released and existing product versions, we have assessed the following relevant to Olympus® products.

As of the time of this letter, Olympus has no evidence of any exploitation of these vulnerabilities affecting the safety or security of the products. Based on our current assessment, we have not identified a patient safety impact. Under certain network access conditions, exploitation could result in unauthorized access to patient information.

Affected Products

Products and Model #	Vulnerability Name
VaultStream™ Server software Versions 10.x and older	**CVE-2022-41089**
	CVE-2023-35390 **CVE-2023-36792** **CVE-2023-36793** **CVE-2023-36794** **CVE-2023-36796** **CVE-2023-44487**

	CVE-2024-21409 **CVE-2024-38229**
	CVE-2021-22117 **CVE-2025-50200**
	CVE-2024-4577

CVSS Scoring Information

CVE ID	CVSS Score	Details
CVE-2022-41089	**7.3**	CVSS:4.0/BE*MAV:L/MAC:L/MAT:P/MPR:H/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H
CVE-2023-35390 **CVE-2023-36792** **CVE-2023-36793** **CVE-2023-36794** **CVE-2023-36796** **CVE-2023-44487** **CVE-2024-21409** **CVE-2024-38229**	**7.3**	CVSS:4.0/BE*MAV:L/MAC:H/MAT:P/MPR:H/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H
CVE-2021-22117 **CVE-2025-50200**	**7.3**	CVSS:4.0/BE*MAV:L/MAC:H/MAT:P/MPR:H/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H
CVE-2024-4577	**7.3**	CVSS:4.0/BE*MAV:L/MAC:H/MAT:P/MPR:H/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H

*CVSS:4.0/BE: Environment Score based on our product environment

Vulnerability Overview

Vulnerability Name	Description
CVE-2022-41089 **.NET Framework Remote Code Execution vulnerability**	**Technical Details:** This is a remote Code Execution vulnerability. When exploited security issues in .NET Framework where restricted mode is triggered for the parsing of XPS files, could potentially allow gadget chains leading to remote code execution. **Potential Impact:** This vulnerability, if exploited, could allow an attacker to execute remote code through the manipulation of XPS file parsing mechanisms.

CVE-2023-35390 **CVE-2023-36792** **CVE-2023-36793** **CVE-2023-36794** **CVE-2023-36796** **CVE-2023-44487** **CVE-2024-21409** **CVE-2024-38229** **.NET and Visual Studio Remote Code Execution Vulnerability**	**Technical Details:** Several remote code execution vulnerabilities in .NET and Visual Studio and can execute an arbitrary code remotely impacting the system and application. **Potential Impact:** This vulnerability, if exploited, can lead to remote code execution.
CVE-2021-22117 **CVE-2025-50200** **Unhardened plugin directory permissions in RabbitMQ for Windows versions prior to 3.8.16 allow local arbitrary plugin injection**	**Technical Details:** If exploited, an attacker can execute arbitrary code on the running RabbitMQ server by adding arbitrary plugins. **Potential Impact:** This vulnerability, if exploited, can lead to remote code execution.
CVE-2024-4577 **PHP-CGI OS Command Injection Vulnerability**	**Technical Details:** If exploited, an attacker can use Windows-based PHPH in CGI mode that contains an OS command injection vulnerability allowing to execute arbitrary code. **Potential Impact:** This vulnerability, if exploited, can lead to remote code execution.

Mitigations:

Olympus recommends that customers implement the following mitigations to reduce potential risk associated with these vulnerabilities.

- Implement firewall rules to detect and block malicious HTTP requests.
- Restrict access to application to authorized IP or user only, limiting exposure to external and internal network.
- Set up enhanced monitoring to detect abnormal HTTP traffic patterns and unusual process trees on the application server.
- Implement firewall rules to inspect and filter out suspicious, large, or malformed requests.

- Configure EDR solutions to monitor for anomalous, high CPU usage, sudden service crashes, or rapid memory consumption on the application server.

As these products are not Internet-facing and access to the hospital network would be required, Olympus recommends alongside the mitigations outlined above that customers continue to follow established cybersecurity best practices and review the General Hardening Guide located on our Global Product Security Website.

https://www.olympus-global.com/products/productsecurity/globalpolicy/product-hardening.html

Next Steps

Should additional mitigations and/or remediations be determined, Olympus will communicate accordingly.

Contact Information

If you have any questions regarding this security advisory, including what version of the VaultStream Server you have or any issue you may have with an Olympus® product, please contact your regional Customer Support Center.

Thank you for your continued partnership and attention to this important matter.