



Date: September 14, 2026
Product: MEDICAL CONTROL UNIT FOR ENDOSURGERY
Model : UCES-4
Subject: Notification of End of Security Support of MEDICAL CONTROL UNIT
FOR ENDOSURGERY UCES-4

Dear Customer:

This letter serves as notification of a change in Olympus' customer support services. The effective date shall be the date of issuance of this letter.

Olympus has discontinued security support for the operating system embedded in the MEDICAL CONTROL UNIT FOR ENDOSURGERY UCES-4 (hereinafter referred to as "UCES-4") firmware. This action is necessary because the operating system embedded in the UCES-4 is no longer supported by its vendor.

Regarding the End of Security Support

Olympus will no longer be able to provide security patches for the OS software should new security vulnerabilities be discovered in the future, due to the OS vendor terminating their support.

As of the date of this notice, Olympus has not identified any critical vulnerabilities affecting this product and is not aware of any cyber-attacks targeting this product.

If we become aware of a critical vulnerability related to Olympus products in the market, we will assess the risk and notify you of any recommended actions.

Until the repair service period for this product expires, we will continue to provide hardware support for such repairs. Additionally, we will provide software updates that are not affected by OS support termination, in order to maintain functionalities (e.g., ensuring compatibility with other products).

Recommendations for Future Cyber-Security Risk Mitigation of the UCES-4

As stated in the IMDRF's Guidance for Medical Device Cybersecurity, stakeholders (e.g., medical device manufacturers (MDM) and healthcare delivery organizations (HDO)) within the healthcare industry have a shared responsibility to provide for the security of medical devices. Olympus recommends that customers continue to follow cybersecurity best practices to secure their environment, such as, but not limited to access-control mechanisms, user procedures, and training to adequately protect medical products from unauthorized access.



Additionally, please consider the following control measures.

- Checking Network Connection

Please verify once again that UCES-4 is not connected to a public network or the hospital network. This product is not designed for use with a network connection.

- Sealing USB ports (MEMORY port, SYSTEM 1 port, SYSTEM 2 port)

Plug in a port lock which cannot be removed without using a dedicated key device (e.g., USB Port Lock, model number: UL03, sold by SmartKeeper or equivalent product), into the MEMORY port on the front of the product and the SYSTEM 1/2 port on the back. Additionally, if a cable is connected, we recommend applying a security seal (e.g., Sanwa Supply Security Seal [Model No.: 200-SL007] or an equivalent product) to the connection point between the cable and the port.

- Sealing LAN ports (SYSTEM I/F 1–6 ports)

Plug in a port lock that cannot be removed without using a dedicated key device (e.g., LAN Port Lock, model number: NL03, sold by SmartKeeper or equivalent product) into the SYSTEM I/F 1–6 ports on the back of the product. Additionally, if a cable is connected, we recommend applying a security seal (e.g., Sanwa Supply Security Seal [Model No.: 200-SL007] or an equivalent product) to the connection point between the cable and the port.

Please note that these are just suggestions and not an exhaustive list of recommendations or security measures that your organization may consider. Olympus does not provide any representations, warranties, or guarantees on the outcome of any cybersecurity measures customers choose to employ.

If you have questions, concerns, please reach out to your Olympus sales representative or Customer Service Center for more information.

Olympus recommends customers to regularly visit our Product Security websites to obtain the latest product security related information.