KARL STORZ SE & Co. KG • Postfach 230 • 78503 Tuttlingen/Germany

July 16th, 2024

Security Notice CVE-2024-30078

CVE-2024-30078 - Windows Wi-Fi Driver Remote Code Execution Vulnerability

Dear Sir or Madam,

KARL STORZ is aware of and currently monitoring the Vulnerability CVE-2024-30078. This vulnerability was disclosed by the Microsoft Corporation on June 11th, 2024 and describes a Wi-Fi Driver Remote Code Execution Vulnerability on various Windows Operating Systems. So far, we can say that KARL STORZ or our customers are not harmed in any way. KARL STORZ will keep investigating that important matter and keep you posted.

Although KARL STORZ had no reports of this vulnerability being exploited on a KARL STORZ product, all versions of the KARL STORZ WD300 AIDA and WD310 AIDA C are WiFi capable and thus potentially affected. By default, the WiFi capability is disabled for both products. If the WiFi capability was manually enabled at a later point in time, the vulnerability may be exploitable.

KARL STORZ recommends the following steps:

Mitigation

- Disable the Wi-Fi feature on all versions of the KARL STORZ AIDA and AIDA C.
- Please refer to the product specific IFU for the detailed steps on how to disable the WiFi capability.

Employ Good Network Hygiene Practices

- Ensure data has been backed up and stored according to your individual processes and disaster recovery procedures.
- Execute updates to malware protection, where available.

For more information on this CVE, please follow the links below:
https://nvd.nist.gov/vuln/detail/CVE-2024-30078
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078

If you have questions, please contact your KARL STORZ sales representative, or contact us at the following address: productsecurity@karlstorz.com.

Revision History

Version	Date	Comment
1.0	2024-07-16	Initial advisory

Annex I - List of products

Article/Model	Product Description	Software Version	Affected by CVE-2024-30078
WD300	AIDA®	All software version	**Affected**
WD310	AIDA® C	All software version	**Affected**