# “Follina” Statement

Publication date: 2022 July 11

*Update A: 2024 December 19*

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities “Follina” affecting the Microsoft Windows Support Diagnostic Tool (MSDT).

## Executive Summary

As detailed in Microsoft Security Advisory on CVE-2022-30190, a vulnerability has been found on the Microsoft Windows Support Diagnostic Tool (MSDT). The vulnerability shows an overall CVSS score of 7.8 which is considered High.

Vulnerability concerns multiple Microsoft operating systems, including server and RT versions.

According to Microsoft, “A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user’s rights.”

The segments of the Fresenius group are actively monitoring “Follina” and analysis actions were taken to determine if any impact on our current products.

## Fresenius products assessment

The following list of products were assessed and **are not affected by "Follina"**.

### Fresenius Kabi

| **Product** | **Versions** |
|---|---|
| • Infusion Pumps – Agilia (Agilia Intuitive Generation and Agilia Connect) | All versions |
| • Infusion Pumps – Exelia | All versions |
| • Infusion Pumps – Orchestra | All versions |
| • Enteral Nutrition Pumps – Amika | All versions |
| • Infusion Pumps – INfusia | All versions |
| • Enteral Nutrition Pumps – Enfusia | All versions |
| • Monitoring Devices – Conox | All versions |
| • Vigilant Software Suite | All versions |
| • Agilia Partner | All versions |
| • Exelia Partner | All versions |
| • Amika Partner | All versions |
| • INfusia Centro | All versions |

Update A

| **Product** | **Versions** |
|---|---|
| Infusion Pump - Ivenix | All Versions |
| Ivenix Infusion Management System (IMS) | All versions |
| Ivenix Infusions Dashboard | All versions |

## "Follina" impact rationale

None of the Microsoft Windows Support Diagnostic Tool "Follina" reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with "Follina":

- CVE-2022-30190

## General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate Medical Devices into IT infrastructure. The Fresenius Group recommends operators of Medical Devices and software to incorporate the following industry best practices into their defense-in-depth strategy:

- Conduct a comprehensive and periodic security risk assessment on the medical network in accordance with operational security best practices such as ISO 27002
- Minimize network exposure for all medical devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius Medical Devices behind firewalls, in dedicated medical networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated medical network
- Implement application firewalls capable of deep packet inspection to help protect against zero-day vulnerabilities and the latest exploits
- Use appropriate authentication and authorization of users on the network
- Implement physical controls that ensure no unauthorized persons would have access to the medical devices and systems
- Ensure that all programming software and equipment (service laptops, etc.) are kept in locked cabinets and are never connected to any network other than the medical network they are intended to service
- Ensure that all portable media used for data exchange with the medical network (such as CDs, USB drives, etc.) are scanned before use
- Implement a process to monitor, prevent and contain malwares and computer viruses.

Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but not limited to: Data Leak, Data Corruption, Data Loss, Network or Service Outage, etc.

## References

Regarding “Follina” more details can be found on:

Microsoft vulnerability details: Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability
NIST NVD details: CVE-2022-30190

## Contacts

For any questions or suggestions please contact your regional marketing manager.