“CVE-2022-45611” vulnerability Statement

Publication date: 2023 November 24th

This document aims to provide information on the assessment of a potential product impact linked with the disclosed vulnerability “CVE-2022-45611”.

Executive Summary

As detailed in CVE-2022-45611, one vulnerability has been found on the Fresenius Kabi product PharmaHelp. The CVE-2022-45611 shows an overall CVSS score of 9.8 which is considered as critical.

The vulnerability concerns one product.

CVE description: *“An issue was discovered in Fresenius Kabi PharmaHelp 5.1.759.0 allows attackers to gain escalated privileges via capture of user login information.”*

The segments of the Fresenius Group are actively monitoring the vulnerabilities impacting the Fresenius products. Analysis actions were taken to confirm the impact of CVE-2022-45611 on our current products.

Fresenius products assessment

The following list of products was assessed and **are affected:**

Fresenius Kabi

Product	**Versions**
PharmaHelp	All versions

CVE-2022-45611 impact rationale

The reported vulnerability CVE-2022-45611 can be exploited on these products.
The potential impact is reading, changing and deletion of PharmaHelp configuration, operator, and master data.

CVE-2022-45611 Cybersecurity recommendations

To mitigate this vulnerability:

- The PharmaHelp system network should be segmented (isolated).
- Only devices which need to have access to the PharmaHelp system should be able to connect to the PharmaHelp server.
- Access to PharmaHelp workstation(s) and terminals should be restricted.
- User accounts which are not required any more should be deleted.

General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate devices into IT infrastructure. The Fresenius Group recommends operators of 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 network in accordance with operational security best practices such as ISO 27002

- Minimize network exposure for all devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius devices behind firewalls, in dedicated networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated 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
- Use complex passwords for all user accounts. Complex passwords should contain a good mixture of upper/lower case letters, numbers, and symbols. Passwords should also not be based on dictionary words and should contain at least ten characters
- Implement physical controls that ensure no unauthorized persons would have access to the 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 network they are intended to service
- Ensure that all portable media used for data exchange with the 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 “CVE-2022-45611” more details can be found on:

MITRE CVD Entry
NVD CVE entry

Contacts

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