FRESENIUS

“Access:7” Statement

Publication date: 2022 June 29

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities “Access:7”.

Executive Summary

As detailed in the ICS advisory ICSA-22-067-01, 7 vulnerabilities have been found in Axeda agent and Axeda Desktop Server by PTC. The ICSA-22-067-01 shows an overall CVSS v3 score of 9.8 which is considered critical.

Vulnerabilities may concern medical devices, Internet of Things (IoT), and embedded devices.

According to ICSA-22-067-01, successful exploitation of these vulnerabilities could result in full system access, remote code execution, read/change configuration, file system read access, log information access, and a denial-of-service condition.

Vulnerabilities are the following: Use of Hard-coded Credentials, Missing Authentication for Critical Function, Exposure of Sensitive Information to an Unauthorized Actor, Path Traversal, Improper Check or Handling of Exceptional Conditions.

The segments of the Fresenius group are actively monitoring “Access:7” 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 "Access:7"**.

Fresenius Medical Care

Product	**Versions**
5008	All versions
5008s	All versions
6008	All versions
Silencia	All versions
SleepSafe Harmony	All versions
BCM – Body Composition Monitor	All versions

"Access:7" impact rationale

None of the "Access:7" reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with "Access:7":

- CVE-2022-25246
- CVE-2022-25247
- CVE-2022-25248
- CVE-2022-25249
- CVE-2022-25250
- CVE-2022-25251
- CVE-2022-25252

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 “Access:7” more details can be found on:

The ICS advisory: ICSA-22-067-01
The PTC Security Advisory: https://www.ptc.com/en/support/article/CS363561

Contacts

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