“NUCLEUS:13” Statement

Publication date: 2021 November 24

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities “NUCLEUS:13”.

Executive Summary

As detailed in ICSA-21-313-03, 13 vulnerabilities have been found on the Siemens Nucleus RTOS by Forescout Research Labs and Medigate. The ICSA-21-313-03 shows an overall CVSS score of 9.8 which is considered critical.

Nucleus is a closed-source real-time operating system (RTOS) used in safety-critical devices, such as anesthesia machines, patient monitors, ventilators, and other healthcare equipment.

According to ICSA-21-313-03, “Successful exploitation of these vulnerabilities could cause a denial-of-service condition, allow an information leakage, or remote code execution”.

Vulnerabilities are the following: Type Confusion, Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements.

The segments of the Fresenius group are actively monitoring “NUCLEUS:13” 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 NUCLEUS:13**.

Fresenius Kabi

Product	**Versions**
• Infusion Pumps – Agilia	All versions
• Infusion Pumps – Exelia	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

"NUCLEUS:13" impact rationale

Fresenius Kabi Devices do not use the affected TCP/IP stack.
None of the "NUCLEUS:13" reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with "NUCLEUS:13":

- CVE-2021-31344
- CVE-2021-31345
- CVE-2021-31346
- CVE-2021-31881
- CVE-2021-31882
- CVE-2021-31883
- CVE-2021-31884
- CVE-2021-31885
- CVE-2021-31886
- CVE-2021-31887
- CVE-2021-31888
- CVE-2021-31889
- CVE-2021-31890

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 “NUCLEUS:13” more details can be found on:

Siemens Security Advisory: SSA-044112
The ICS advisory: ICSA-21-313-03

Contacts

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