FRESENIUS

“INFRA:HALT” Statement

Publication date: 2021 October 12

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

Executive Summary

As detailed in ICSA-21-217-01, 14 vulnerabilities have been found on HCC Embedded InterNiche TCP/IP stack, previously known as InterNiche NicheStack. The ICSA-21-217-01 shows an overall CVSS score of 9.8 which is considered critical.

According to ICSA-21-217-01, Successful exploitation of these vulnerabilities may result in unauthorized access to arbitrary information, DNS cache poisoning, remote code execution, or a denial-of-service condition.

Vulnerabilities are the following: Return of Pointer Value Outside of Expected Range, Improper Handling of Length Parameter Inconsistency, Use of Insufficiently Random Values, Improper Input Validation, Uncaught Exception, Numeric Range Comparison Without Minimum Check, Generation of Predictable Numbers or Identifiers, Improper Check or Handling of Exceptional Conditions, Improper Null Termination.

The segments of the Fresenius group are actively monitoring “INFRA:HALT” 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 INFRA:HALT**.

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

"INFRA:HALT" impact rationale

These products are not using the affected TCP/IP stack.
None of "INFRA:HALT" reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with "INFRA:HALT":

- CVE-2020-25767
- CVE-2020-25928
- CVE-2020-25927
- CVE-2020-25926
- CVE-2020-35683
- CVE-2020-35684
- CVE-2020-35685
- CVE-2021-31400
- CVE-2021-31401
- CVE-2021-31226
- CVE-2021-31227
- CVE-2021-31228
- CVE-2021-27565
- CVE-2021-36762

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 "INFRA:HALT" more details can be found on:

- The coordinated disclosure publication: https://www.forescout.com/resources/infrahalt-discovering-mitigating-large-scale-ot-vulnerabilities/
- HCC Advisory: https://www.hcc-embedded.com/newsletter/interniche-nichestack-vulnerabilities-updates
- The ICS CERT advisory: HCC Embedded InterNiche TCP/IP stack, NicheLite (Update A) | CISA

Contacts

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