# “Ripple20” Statement

Publication date: 2020 July 06

Update A: 2020 July 09

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities “Ripple20”.

## Executive Summary

As detailed in the CISA Advisory ICSA-20-168-01, 19 vulnerabilities have been found on a TCP/IP stack developed by Treck Inc. The ICSA-20-168-01 shows an overall CVSS score of 10.0 which is the highest possible and considered critical.

Vulnerabilities concern some medical devices which utilize the Treck TCP/IP stack to communicate data with communication networks.

According to the CERT Coordination Center – VU#257161 – “The impact of these vulnerabilities will vary due to the combination of build and runtime options used while developing different embedded systems. This diversity of implementations and the lack of supply chain visibility has exacerbated the problem of accurately assessing the impact of these vulnerabilities. In summary, a remote, unauthenticated attacker may be able to use specially-crafted network packets to cause a denial of service, disclose information, or execute arbitrary code”.

Vulnerabilities are the following: Improper Handling of Length Parameter Inconsistency, Improper Input Validation, Double Free, Out-of-bounds Read, Integer Overflow or Wraparound, Improper Null Termination, Improper Access Control.

The segments of the Fresenius group are actively monitoring “Ripple20”, 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 "Ripple20"**.

### 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 |

Update A

### Fresenius Medical Care

| **Product** | **Versions** |
|---|---|
| 4008S | All versions |
| UniDataLink | All versions |

## Ripple20 impact rationale

The listed products are not using the Treck Inc. TCP/IP stack.
None of "Ripple20" reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with "Ripple20":

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905
- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912
- CVE-2020-11913
- CVE-2020-11914

## 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 “Ripple20” more details can be found on:

ICS advisory: ICSA-20-168-01
Treck dedicated webpage: https://treck.com/vulnerability-response-information/
JSOF webpage: https://www.jsof-tech.com/ripple20/
The CERT Coordination Center Advisory: https://kb.cert.org/vuls/id/257161

## Contacts

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