HMS Security Advisory – Ripple20 vulnerabilities

HMSSAR-2020-06-23-001

Publication date: 23 June 2020
Last update: 14 October 2020

Overview

The JSOF research lab has discovered 19 different vulnerabilities in the third-party TCP/IP software library developed by company Treck Inc. This information was disclosed publicly on June 16 by JSOF.

While most HMS products are not using this software library some older products are affected. We are currently investigating the impact of these vulnerabilities, which are depending of software library version and the actual product configuration.

As soon as we have updated information about vulnerabilities, and recommended countermeasures, per product, we will post information on our Security Advisory page:

https://www.hms-networks.com/cybersecurity

Impact

Under specific circumstances, it may be possible that these vulnerabilities could lead to a remote code execution via a network-based attack without authentication, or denial of service (DoS), or information disclosure.

Since the detected vulnerabilities are related to TCP/IP communication, products without Ethernet or WLAN connection are not affected.

HMS Recommendations

Monitor HMS Security Advisory page which is updated as soon as new information is available about affected products.

In case you are sourcing a custom developed product from HMS, contact us for additional information.

Use firewalls and do not directly expose the device on internet.

In addition, the CERT Coordination Center at Carnegie Mellon University recommend a series of mitigation actions to block and detect anomalous IP traffic, we recommend using such protection, if possible, to minimize the attack surface of networked devices.

See: https://kb.cert.org/vuls/id/257161

HMS Industrial Networks AB, PO Box 4126, 300 04 Halmstad, Sweden
Tel. +46 35 17 29 00, www.hms-networks.com

HMS products confirmed unaffected by Ripple20 vulnerabilities

The following product families are not vulnerable:

- Anybus Embedded Devices (Anybus-S, Anybus-IC, Anybus-CC, Anybus-M)
- Anybus X-gateway
- Anybus-Communicator
- Anybus Edge Gateway
- Anybus M-Bus to Modbus TCP gateway
- Anybus Wireless Bridge II
- Anybus Wireless Bolt
- Anybus Wireless Bolt IoT
- Anybus Switches & Routers (AWB5xxx)
- Anybus WLAN Access Points (AWB4xxx)
- Gateway family com.tom INDUSTRY (e.g. CTI 100.DIO8.W or CTI 140.MIO12.C)
- IPC@CHIP Family SC1x5
- IXXAT branded products
- Intesis protocol converters
- Ewon Flexy products
- Ewon Cosy 131
- Ewon Cosy 141 (No vulnerabilities of medium or high severity, CVSS score > 6.9)
- Ewon CD-series (No vulnerabilities of medium or high severity, CVSS score > 6.9)
- Ewon Netbiter 100, 200 and 300-series

The list will be supplemented when products are confirmed unaffected

HMS Industrial Networks AB, PO Box 4126, 300 04 Halmstad, Sweden
Tel. +46 35 17 29 00, www.hms-networks.com