HMS Security Advisory Report – Log4Shell and Anybus

HMSSAR-2021-12-14-001

Publication date: 14 December 2021
Last update: 20 December 2021

Overview
On December 9th, 2021, a 0-day exploit in the Java logging library log4j (version 2) published as CVE-2021-44228, (critical CVSSv3 10) was divulged.
We are currently investigating the potential impact of these vulnerabilities for our Anybus branded products, currently no investigated product has used the vulnerable component.

Impact
An affected product may be vulnerable to remote Code Execution (RCE) by logging a certain string.

HMS Anybus products confirmed unaffected by Log4Shell 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 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)
- Anybus Edge Gateway
- Gateway family com.tom INDUSTRY (e.g. CTI 100.DIO8.W or CTI 140.MIO12.C)
- IPC@CHIP Family SC1x5

The list will be supplemented when products are confirmed unaffected.

HMS Anybus tools confirmed unaffected by Log4Shell vulnerabilities
The following tools are not vulnerable:

- HMS IPconfig
- HMS Firmware Manager II
- Certificate Generator
- PROFINET GSD Generator
- ABCC40 EDS Generator
- ACM IIoT
- ACM CANopen
- ACM X-gateway
- ACM Generic CAN
- ACM RS232/RS422/RS485
- ACM PROFiBUS
- ACM DeviceNet

The list will be supplemented when tools are confirmed unaffected.
HMS Recommendations

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

Additional information