Cyber Security Statement

Update Log4j on Lenze Products (No. 3)

2022-01-14

Currently (as of Jan. 14, 2022), we can confirm for the following Lenze products that they are not affected by the Log4j vulnerability when shipped. The products highlighted, marked with an asterix, are new additions.

More products are under review, so we will continuously expand this list.

- 8400
- 9300
- 9400
- 32xxC
- c250-S
- c300
- c5x0
- *c7x0
- *DSD (Drive Solution Designer)
- Easy UI-Designer
- EASY Starter Suite
- *Engineer
- *i400
- *i500 Note: Check WLAN module still open
- i700
- i950
- p300
- p500
- PLC-Designer V3
- *v200
- *VisiWinNet
- x4-Remote
- x5x0

We have on 2022-01-14 checked whether the listed product(s) is affected by descriped malware with the help of manual inspection. The result of this check was negative

Reference: SysE-18033