Cyber Security Statement

Log4j on Lenze products

2021-12-17

Recently it became known that Log4j has a vulnerability, whereupon hackers and cyber security specialists are now in a race to break into computer systems and prevent it.

Log4j is software that logs what happens inside a Java application. Java is a programming language. Log4j is used in a variety of Java based applications due to its sophistication and configurability. On December 10th, 2021, a vulnerability (CVE-2021-44228) in Log4j was disclosed that makes it very easy for attackers to attack and take over systems that use Log4j. Due to the widespread use of Log4j and the ease with which the vulnerability can be exploited, this has also been widely reported in the press.

Log4j-Sicherheitslücke: Ungeschützt | ZEIT ONLINE
https://www.zeit.de/digital/2021-12/log4j-sicherheitsluecke-software-log4shell-it

Log4j-Sicherheitslücke: Wie löscht man ein brennendes Internet? - DER SPIEGEL
https://www.spiegel.de/netzwelt/web/log4j-sicherheitsluecke-wie-loescht-man-ein-brennendes-internet-a-27729847-8e28-4187-b4a2-468a45137fb4

As a result, bhn has implemented measures to protect our Lenze IT infrastructure. It is monitoring developments and will implement further measures if necessary.

In this context, you can share the following information with customers:
Currently (as of 12/17/2021), we can confirm for the following Lenze products, that they are not affected by the Log4j security vulnerability when shipped:

- 8400
- 9300
- 9400
- 32xxC
- c250-S
- c300
- c5x0
- Easy UI-Designer
- EASY Starter Suite
- i700
- i950
- p300
- p500
- PLC-Designer V3
- x4-Remote
- x5x0

We have on 2021-12-17 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-18719