Safety alert

BSI cyber security alert regarding the Log4j Java library

When operating devices or components of machinery that are connected to a network and contain software elements with security vulnerabilities (here: the Log4j Java library ('Log4Shell')), users may be at risk due to malfunctioning or non-functioning software-controlled safety systems!

An IT security service provider has disclosed the 'Log4Shell' vulnerability of the widely used Log4j logging library for Java applications. This library is used to create log files in numerous Java applications. Therefore, safety-critical systems can also be affected, either directly or due to components that are part of their setup or supplementary programs required for their operation (control devices, control panels, virtualisation software, etc.). As a result, numerous manufacturers have already published security information regarding their products (e.g. Siemens, Schneider Electric, Rockwell Automation).

The Federal Office for Information Security (BSI) has categorised the threat as extremely critical (highest level 4/red).

Measures:

- *Check whether any devices and machinery utilised in your unit use the Log4j Java logging library. This applies to both purchased standard devices and machinery and custom-made solutions.*
- *Immediately shut down any affected devices and machinery that are not essential.*
- *Mark these devices as out of order ('defekt') or requiring inspection ('zu prüfen') and safeguard them against being put into operation inadvertently (e.g. lock the main switch, put adhesive tape around the plug or tie a bag around it – see Figure 1).*
- *In the case of affected devices and machinery that cannot be shut down, check whether the safety-relevant features (e.g. pressure/temperature monitoring, light barriers, locking mechanisms of protective covers) run properly at every use.*
- *Additional protective measures (e.g. barriers, safety distance, auxiliary tools) may be necessary for checking the safety features.*
- *Have the software of all affected devices and machinery examined and, if necessary, updated in accordance with guidance from the manufacturers.*

Please note:

The BSI cyber security alert contains links to various guides, solutions, workarounds and software updates from the manufacturers mentioned above, among others. Other manufacturers will probably provide similar support. Contact the relevant manufacturer or provider for information.

UNIVERSITÄT DUISBURG ESSEN

Open-Minded

Arbeitssicherheit

[1] Example of a simple way of marking devices as out of order ('defekt' in German)

BSI cyber security alert
https://kurzelinks.de/BSICSW-Log4Shell

Technical information on critical vulnerabilities of engines and machinery (in German) from the Institute for Occupational Safety and Health (IFA) of the German Social Accident Insurance (DGUV)
https://kurzelinks.de/DGUVIFA-Log4Shell

2021-12-21, page 1 of 1