

“Actually the world is still facing the security problem due to “log4j logging”

Please find below an amended version of our statement considering the latest customer requests.

Still valid: The usage of MAGMASOFT® does not cause a vulnerability.

Please find below our actual statement based on the actual knowledge.

The statement will also be available in the support area of our website:

MAGMA Statement Log4j-Vulnerability Date of status: January 14, 2022

[CVE-2021-44228¹](#)

MAGMASOFT® 5.4 and MAGMASOFT® 5.5 use the "Log4j 1.2.17" library. The versions "1.x" are not directly affected by the [CVE-2021-44228¹](#) security vulnerability.

The security vulnerability [CVE-2021-44228¹](#) can only be exploited in "Log4j 1.x", if JNDI is used in the Log4j configuration. MAGMASOFT® does not use JNDI and is therefore not vulnerable based on the currently available information.

[CVE-2019-17571²](#)

The older security vulnerability [CVE-2019-17571²](#) in "Log4j 1.x" can be exploited if unrestricted logging from remote clients is accepted. MAGMASOFT® does not accept logging from remote clients and is therefore not vulnerable with currently available information.

[CVE-2021-4104³](#)

In order to exploit the [CVE-2021-4104³](#) vulnerability in Log4j 1.x, an attacker would need to obtain write permissions to the MAGMASOFT® installation and modify the stored file log4j.properties in a way that the functions of the JMSAppender class are used. MAGMASOFT® has not activated these functions.

Therefore, according to the present situation, no further measures are required for the operation of MAGMASOFT®.

References:

[1] <https://www.cvedetails.com/cve/CVE-2021-44228/>

[2] <https://www.cvedetails.com/cve/CVE-2019-17571/>

[3] <https://www.cvedetails.com/cve/CVE-2021-4104>

[4] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=8 (only in german) ”