

Manufacturers Declaration

MICROSENS GmbH & Co. KG
Küferstraße 16
D-59067 Hamm / Germany

Hamm, December 14th, 2021

CVE-2021-44228 (log4j) vulnerability

Summary

MICROSENS java-based software products (mainly NMP and SBM, see Appendix B for details) incorporate the log4j library, but are not affected by the vulnerability, as JNDI and LDAP services that are the root cause of the vulnerability are not used.

Description

Software using the Apache Log4j2 library up to version 2.14.1 may be affected by attacks generating arbitrary code execution on the system. This vulnerability is caused by the JNDI/LDAP interface of the library.

From the CVE description [MITRE]:

Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled[..].

Status

All MICROSENS products do not use the JNDI/LDAP interface of the log4j library and therefore do not exhibit the vulnerability (for detailed product list see Appendix B).

Required Actions

None.

Recommended Actions

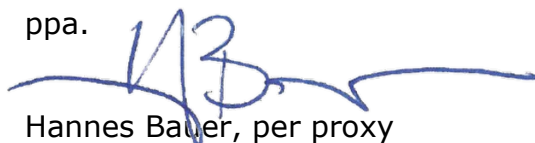
As recommended by all references, preventive actions can be taken to disable functions causing the vulnerability in existing installations (for details see Appendix A: [APACHE]).

When using NMP version 2.5.5 or above, the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS can be set to true to disable the critical behavior of the log4j library.

We are preparing updates of the respective NMP and SBM software products incorporating the log4j library version 2.15.0, that is not affected by the vulnerability.

MICROSENS GmbH & Co. KG

ppa.



Hannes Bauer, per proxy
Technical Director

CVE-2021-44228 (log4j) vulnerability

Appendix A: References

- [MITRE] <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>
- [NIST] <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>
- [BSI] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3
- [APACHE] <https://logging.apache.org/log4j/2.x/security.html>

CVE-2021-44228 (log4j) vulnerability

Appendix B: Products Concerned

Product	Version	Library used	Status
NMP Professional Enterprise	up to 2.5	log4j 1.x	Not affected by vulnerability, as JNDI and JMS Appender are not used
	2.5.5 to 2.9.3	log4j 2.13.3	Not affected by vulnerability, as JNDI and JMS Appender are not used
	2.9.4	log4j 2.15.0	Not affected by vulnerability, fixed log4j library
SBM	1.x	log4j 1.x	Not affected by vulnerability, as JNDI and JMS Appender are not used
	2.0 to 2.8	log4j 1.2.14	Not affected by vulnerability, as JNDI is not used
	2.90 to 2.10.x	log4j 2.13.3	Not affected by vulnerability, as JNDI is not used
	2.11.0 XB2 and above	log4j 2.15.10	Not affected by vulnerability, fixed log4j library
	2.11.0 XB3 and above	Java standard logging only	Not affected, log4j library not used
Switch IP Config Tool	all versions	none	Not affected, log4j library not used
Activation Key Request Generator	all versions	none	Not affected, log4j library not used