Nexans switch firmware, manager and Apache "log4j" vulnerability

KD1824E0

Vulnerability background

Log4j is a popular logging library for Java applications. It is used for high-performance aggregation of log data from an application.

The blog of a service provider for IT security [LUN2021] reports on the vulnerability CVE-2021-44228 [MIT2021] in log4j in versions 2.0 to 2.14.1, which allows attackers to execute their own program code on the target system and thus the server to compromise. This risk arises if log4j is used to log a character string controlled by the attacker, such as the HTTP user agent.

A proof-of-concept (PoC) of the vulnerability was published on Github [GIT2021a] and shared on Twitter [TWI2021]. In addition to the PoC, there are also examples of scripts that randomly examine systems for vulnerability [GIT2021b]. Scripts of this type cannot give administrators any security about the vulnerability, but allow attackers to carry out rudimentary scans for vulnerable systems at short notice.

This critical weak point may have an impact on all Java applications that can be accessed from the Internet and that log parts of the user inquiries with the help of log4j.

For more information see BSI document CVE-2021-44228

Nexans switches unaffected

Nexans is NOT exposed to the Apache "log4j" vulnerability.

All types of Nexans switch firmware and manager software versions are unaffected because Nexans doesn't use Java or the log4j logging library.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 13.12.2021, Mönchengladbach Germany