Legnago, 15 February 2022

Critical vulnerability in Apache Log4j library

Subject: CVE-2021-44228, also named Log4Shell is a Remote Code Execution (RCE) class vulnerability.

CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack.

Updated on 16/December/2021

The latest firmware version **3.15**, available for Netman 204 do not use Log4j at all and are therefore not affected by CVE-2021-44228 and CVE-2021-45046.

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.

What makes CVE-2021-44228 especially dangerous is ease of exploitation: even an inexperienced hacker can successfully execute an attack using this vulnerability. According to the researchers, attackers only need to force the application to write just one string to the log, and after that they are able to upload their own code into the application due to the message lookup substitution function.

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 restricts JNDI LDAP lookups to localhost by default.

Riello UPS ensure his customers that **Log4J library is no more used on NetMan 204 card** therefore it is now immune to CVE-2021-44228 and CVE-2021-45046.

Massimo Zampieri

Single Phase PM

RPS S.p.A.