Mitigation of CVE-2021-44228: potential log4j remote code execution through JNDI vulnerability.

Ghent, 14/12/2021.

Limecraft has assessed the impact of this vulnerability, in particular with regard to the use of the Apache log4j software framework with impacted versions 2.0 to 2.14 in Limecraft Flow components based on Java JVM technologies. Access log analysis covering the past week and up to the deployment of relevant mitigations has not indicated any exploitation of the vulnerability in the components identified below.

The following components in the Limecraft Flow software stack have been found impacted by this vulnerability:

Component	Impact	Mitigation
SOLR 7.6.0, depends on org.apache.logging.log4j version 2.11.0.	**HIGH** This component, which acts as the Limecraft Flow search index is vulnerable should it ever output a log message with a string that triggers the vulnerability and remote code access. The likelihood of this happening in practice is small for the following reasons: • SOLR searches and updates can only be triggered by users registered and logged in to the platform, any other call to the API parts that deal with the search index will not be authorized. • Automated scanning tools are not authenticated against the platform and will be bounced either by the load-balancing layer which is not Java/log4j-based (returning HTTP error codes) or by the application server before being submitted to SOLR. • Any attempt to address SOLR directly by users logged in to the platform would	Use of the `-Dlog4j2.formatMsgNoLookups=true` as an argument to the SOLR Java VM to disable JNDI lookups in log4j logging, as recommended by https://solr.apache.org/news.html This change has been rolled out on 14/12/2021 to all Limecraft Flow deployments. This was done without downtime as all SOLR indices are deployed in a redundant and highly available fashion.

	require a specially crafted search query, which would be traceable in the logs collected from various components in the Limecraft Flow software stack. Limecraft has not found any such attempts in the access logs collected to date.	
Application Server (‘mojito’), deployed with, but not depending on, org.apache.logging.log4j version 2.11.0.	**LOW** The application server that uses the SOLR index searching and updating SOLR documents uses an Apache-provided software library to facilitate this functionality. This library is deployed with the application server along with an impacted version of log4j but it is disabled and not used in any way, as the logback framework is used for logging in Limecraft flow application servers.	The inactive log4j dependency will be removed or updated to at least version 2.15 in a future version of the Limecraft Flow application server. Even though it is inactive, it will still be updated to avoid any impact by yet unknown exploitation methods in the future.