How to mitigate the Log4Shell (CVE-2021-44228, CVSSv3 10.0) vulnerability

Log4Shell

On December 9th, 2021, a 0-day exploit in the popular Java logging library log4j was discovered that results in Remote Code Execution (RCE) by logging a certain string.

The impact of this vulnerability is quite severe. More about this issue impact (somewhere called Log4Shell) might be found at https://www.randori.com/blog/cve-2021-44228/.

What is affected

The VIVO core source code is **not** impacted by this vulnerability, but the Solr platform used by VIVO might be. The following versions of Solr are affected: 7.4.0 to 7.7.3, 8.0.0 to 8.11.0 (source: https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228).

Mitigation

Any of the following are enough to prevent this vulnerability for Solr servers:

- Upgrade to `Solr 8.11.1` or greater (when available), which will include an updated version of the Log4J dependency.
- If you are using Solr's official docker image, no matter the version, it has already been mitigated. You may need to re-pull the image.
- Manually update the version of Log4J on your runtime classpath and restart your Solr application.
- (Linux/MacOS) Edit your `solr.in.sh` file to include: `SOLR_OPTS="$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true"`
- (Windows) Edit your `solr.in.cmd` file to include: `set SOLR_OPTS=%SOLR_OPTS% -Dlog4j2.formatMsgNoLookups=true`
- Follow any of the other mitgations listed at https://logging.apache.org/log4j/2.x/security.html