FOSSA

# Log4Shell Remediation Guide

## DETECT

Find Log4J in your code, with no FOSSA account required:

- **With FOSSA CLI directly (bit.ly/fossa-cli)**

  `fossa log4j`

- **With FOSSA CLI directly (bit.ly/fossa-cli) and jq**

  `fossa analyze . -o | jq . | grep 'log4j-core'`

  Log4J is present if grep finds and print matches

- **With FOSSA Enterprise**

  Learn more about FOSSA: sales@fossa.com

1

## UPGRADE

Where possible, upgrade Log4J to 2.16.0 or higher

- **Direct Dependency:** Upgrade Log4J directly to `2.16.0`
- **Transitive Dependency:** Determine which dependencies rely on Log4J (FOSSA can help) and update them to a version that uses Log4J or higher

Note: Upgrading to `2.17.0` will also resolve a DoS vulnerability (`CVE-2021-45105`)

2

## REMOVE

**Remove problematic classes** from your deployments using the following command (`-q` enables quiet mode, this can be disabled):

```
zip -q -d log4j-core-*.jar
org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

Also remove: `JndiManager, JMSAppender, SMTPAppender`

These changes require **restarting the JVM.**

3

## DISABLE

You can **disable JNDI lookups** by setting the system property `LOG4J_FORMAT_MSG_NO_LOOKUPS` to true or setting an environment variable `log4j2.formatMsgNoLookups` to `true`.

**Note:** JNDI lookups are disabled by default in version `2.16.0+`

Using JDK settings such as changing `trustURLCodebase` is no longer considered an effective mitigation.

4