

# Eurotherm Data Reviewer Log4shell (CVE-2021-44228) Mitigation Instructions

## Contents

Introduction .....	1
Update Instructions .....	1
Login.....	1
Install 7-zip.....	1
Update instructions for Reviewer V3.0.x.....	1
Stop Reviewer.....	2
Remove JndiLookup.class from log4j-core-2.11.1.jar.....	2
Restart Reviewer.....	2
Update instructions for Reviewer V2.1.x.....	2
Stop Reviewer.....	2
Remove JndiLookup.class from log4j-core-2.11.1.jar.....	3
Restart Reviewer.....	3
Update instructions for Reviewer V2.0.1 and earlier .....	3
Stop Reviewer.....	3
Remove JndiLookup.class from log4j-core-2.9.1.jar.....	3
Restart Reviewer.....	4

## Introduction

These instructions cover the Eurotherm Data Reviewer updates required to fully mitigate the log4shell vulnerability. They cover multiple versions of Reviewer, which differ slightly due to the version of Elasticsearch they install. Please check carefully which version of Reviewer you are using.

## Update Instructions

### Login

Login to the Reviewer server with Admin privileges

### Install 7-zip

Download and install the '64-bit Windows x64' version of 7-zip from...

- <https://www.7-zip.org/download.html>

### Update instructions for Reviewer V3.0.x

Reviewer V3.0.x uses Elasticsearch 7.12.1

## Stop Reviewer...

1. Open Windows Services dialog
2. Double click on 'Reviewer API+SPA Service' to open Properties dialog and stop the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and stop the service
4. Double click on 'Elasticsearch 7.12.1 (ES7)' to open Properties dialog and stop the service

## Remove JndiLookup.class from log4j-core-2.11.1.jar

1. Open a command prompt with 'Run as administrator'
2. Change directory...

```
cd C:\Program Files\Eurotherm\Eurotherm Reviewer\ElasticSearch-7.12.1\lib
```

3. Edit log4j-core-2.11.1.jar

```
"C:\Program Files\7-Zip\7z.exe" d log4j-core-2.11.1.jar JndiLookup.class -r
```

4. Check the output should show one file deleted

```
7-Zip 21.06 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-11-24
```

```
Open archive: log4j-core-2.11.1.jar
```

```
--
```

```
Path = log4j-core-2.11.1.jar
```

```
Type = zip
```

```
Physical Size = 1607947
```

```
Updating archive: log4j-core-2.11.1.jar
```

```
Delete data from archive: 1 file, 2937 bytes (3 KiB)
```

```
Keep old data in archive: 75 folders, 1073 files, 3528327 bytes (3446 KiB)
```

```
Add new data to archive: 0 files, 0 bytes
```

```
Files read from disk: 0
```

```
Archive size: 1606391 bytes (1569 KiB)
```

```
Everything is Ok
```

## Restart Reviewer...

1. Open Windows Services dialog
2. Double click on 'Elasticsearch 7.12.1 (ES7)' to open Properties dialog and start the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and start the service
4. Double click on 'Reviewer API+SPA Service' to open Properties dialog and start the service

## Update instructions for Reviewer V2.1.x

Reviewer V2.1.x uses Elasticsearch 7.7.1

## Stop Reviewer...

1. Open Windows Services dialog
2. Double click on 'Reviewer API+SPA Service' to open Properties dialog and stop the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and stop the service
4. Double click on 'Elasticsearch 7.7.1 (ES7)' to open Properties dialog and stop the service

Remove JndiLookup.class from log4j-core-2.11.1.jar

1. Open a command prompt with 'Run as administrator'
2. Change directory...

```
cd C:\Program Files\Eurotherm\Eurotherm Reviewer\ElasticSearch-7.7.1\lib
```

3. Edit log4j-core-2.11.1.jar

```
"C:\Program Files\7-Zip\7z.exe" d log4j-core-2.11.1.jar JndiLookup.class -r
```

4. Check the output should show one file deleted

```
7-Zip 21.06 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-11-24
```

```
Open archive: log4j-core-2.11.1.jar
```

```
--
```

```
Path = log4j-core-2.11.1.jar
```

```
Type = zip
```

```
Physical Size = 1607947
```

```
Updating archive: log4j-core-2.11.1.jar
```

```
Delete data from archive: 1 file, 2937 bytes (3 KiB)
```

```
Keep old data in archive: 75 folders, 1073 files, 3528327 bytes (3446 KiB)
```

```
Add new data to archive: 0 files, 0 bytes
```

```
Files read from disk: 0
```

```
Archive size: 1606391 bytes (1569 KiB)
```

```
Everything is Ok
```

Restart Reviewer...

1. Open Windows Services dialog
2. Double click on 'Elasticsearch 7.7.1 (ES7)' to open Properties dialog and start the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and start the service
4. Double click on 'Reviewer API+SPA Service' to open Properties dialog and start the service

Update instructions for Reviewer V2.0.1 and earlier

Reviewer V2.0.1 and earlier use Elasticsearch 5.6.5

Stop Reviewer...

1. Open Windows Services dialog
2. Double click on 'Reviewer API+SPA Service' to open Properties dialog and stop the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and stop the service
4. Double click on 'Elasticsearch 5.6.5 (elasticsearch-service-x64)' to open Properties dialog and stop the service

Remove JndiLookup.class from log4j-core-2.9.1.jar

1. Open a command prompt with 'Run as administrator'
2. Change directory...

```
cd C:\Program Files\Eurotherm\Eurotherm Reviewer\ElasticSearch\lib
```

3. Edit log4j-core-2.9.1.jar

```
"C:\Program Files\7-Zip\7z.exe" d log4j-core-2.9.1.jar JndiLookup.class -r
```

4. Check the output should show one file deleted

```
7-Zip 21.06 (x64) : Copyright (c) 1999-2021 Igor Pavlov : 2021-11-24
```

```
Open archive: log4j-core-2.9.1.jar
```

```
--
```

```
Path = log4j-core-2.9.1.jar
```

```
Type = zip
```

```
Physical Size = 1549865
```

```
Updating archive: log4j-core-2.9.1.jar
```

```
Delete data from archive: 1 file, 2937 bytes (3 KiB)
```

```
Keep old data in archive: 66 folders, 1028 files, 3394920 bytes (3316 KiB)
```

```
Add new data to archive: 0 files, 0 bytes
```

```
Files read from disk: 0
```

```
Archive size: 1548309 bytes (1513 KiB)
```

```
Everything is Ok
```

Restart Reviewer...

1. Open Windows Services dialog
2. Double click on 'Elasticsearch 5.6.5 (elasticsearch-service-x64)' to open Properties dialog and start the service
3. Double click on 'Reviewer Client Service' Service to open Properties dialog and start the service
4. Double click on 'Reviewer API+SPA Service' to open Properties dialog and start the service