

AmberFin ‘Log4j’ LogPatcher

AmberFin LogPatcher has been issued in response to the Log4j v2 Remote Code Execution vulnerability: <https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know>

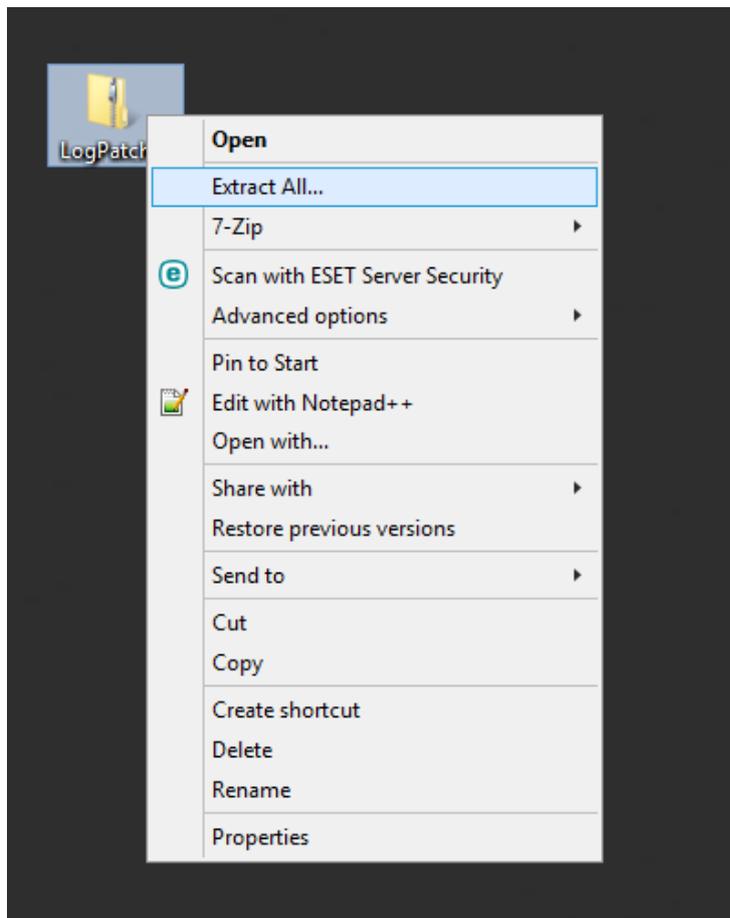
AmberFin uses an earlier version of log4j (v1), which is not vulnerable to this exploit but versions incorporate log4j v2 jars (log4j-core) that are in the affected range of versions (2.7.x - 2.14.x) and are included in third party dependencies.

Dalet is in the process of upgrading all logging in the AmberFin product to log4j v2.17.0 or greater for all future releases.

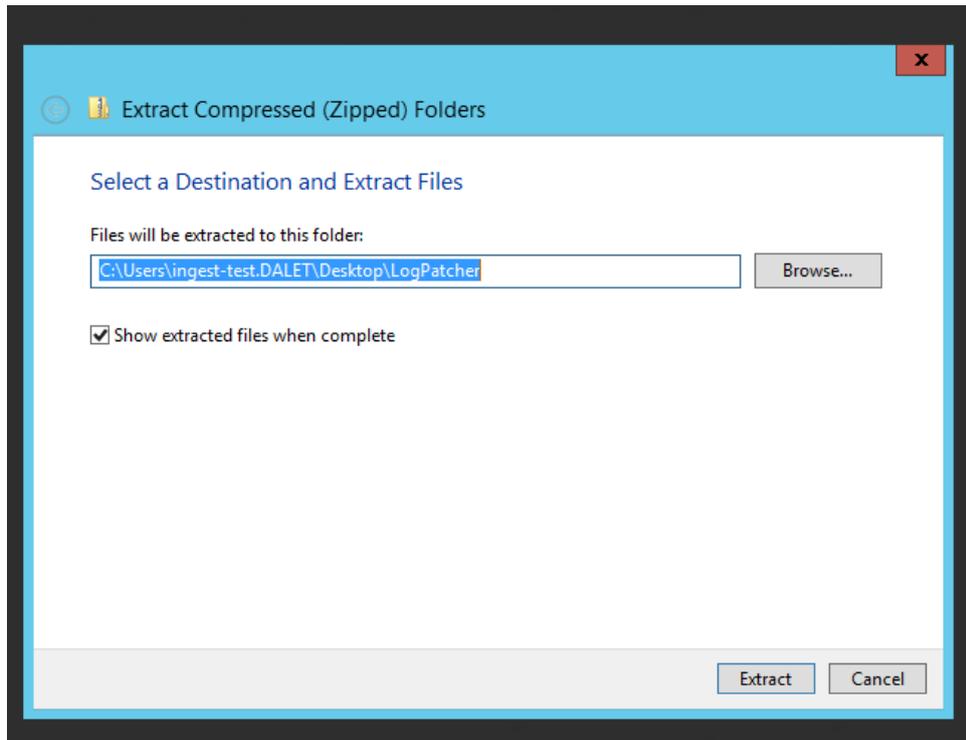
Meantime, customers can patch current and legacy versions of AmberFin using the LogPatcher tool, which will remove completely the jndilookup class from the installation and makes it impossible to run the exploit.

Running LogPatcher

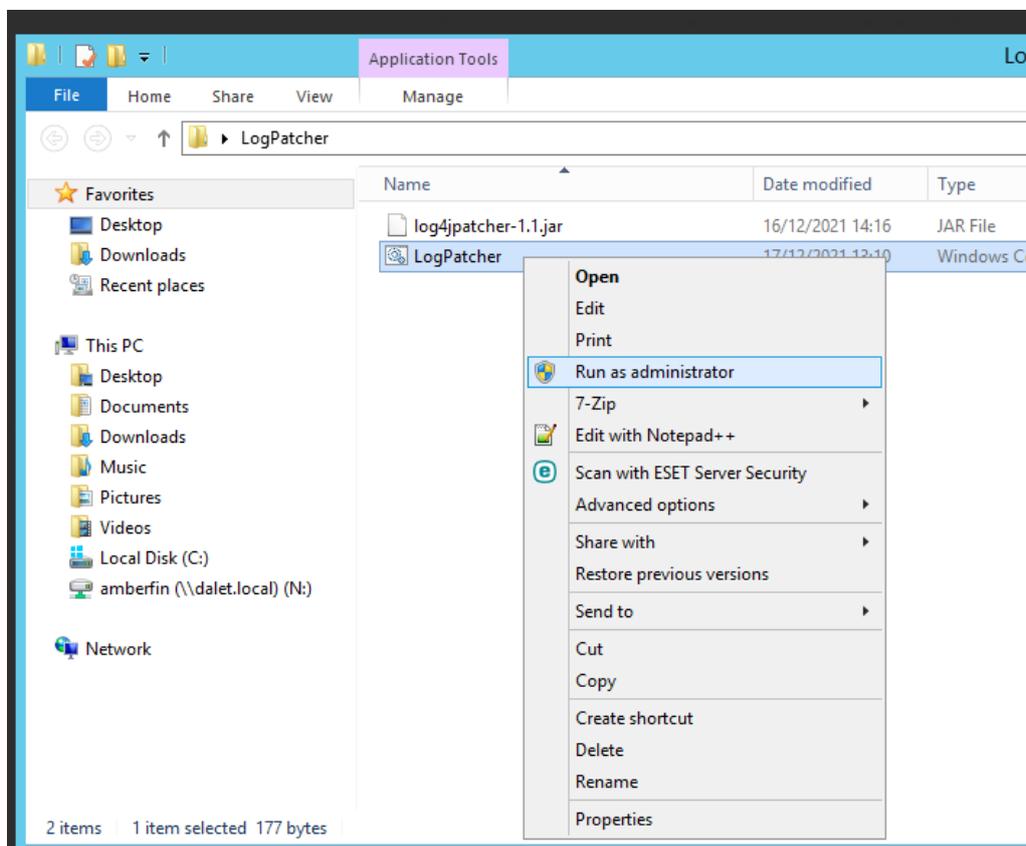
1. Extract or Unzip the **LogPatcher.zip** file anywhere on the AmberFin installed server by right-clicking on the LogPatcher.zip file and clicking ‘**Extract All**’.



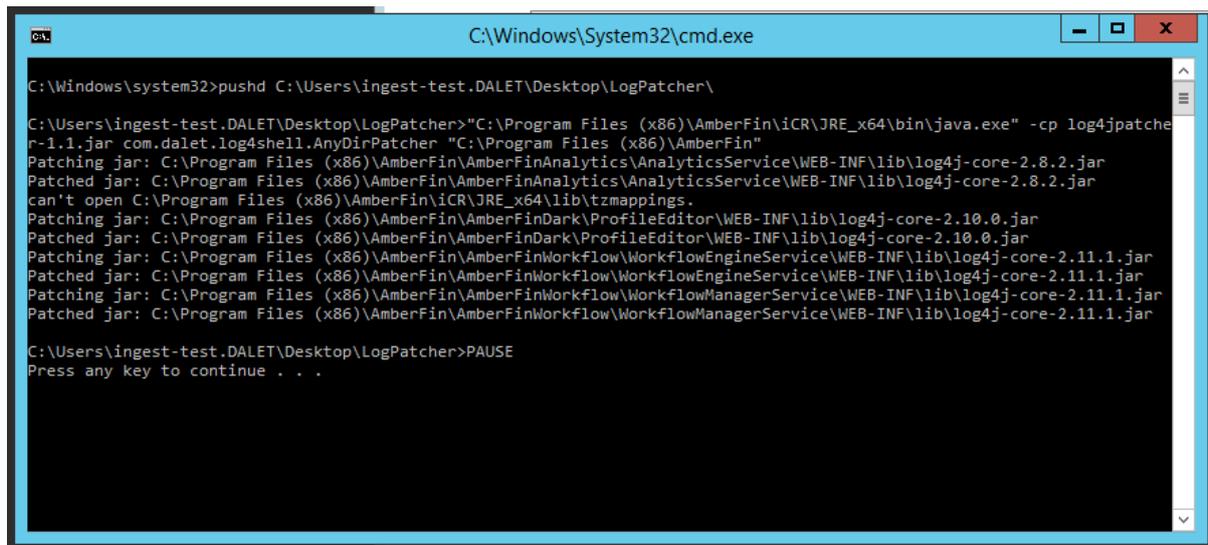
2. Open the installed folder in Windows Explorer, which may open automatically after extracting.



3. Right click on **LogPatcher.cmd** and select '**Run as Administrator**' from the menu then click '**Yes**' in the User Account Control dialog to allow the command to run.



4. A Command Window will open up to report the patching process.



```
C:\Windows\System32\cmd.exe

C:\Windows\system32>pushd C:\Users\ingest-test.DALET\Desktop\LogPatcher\

C:\Users\ingest-test.DALET\Desktop\LogPatcher>"C:\Program Files (x86)\AmberFin\iCR\JRE_x64\bin\java.exe" -cp log4jpatcher-1.1.jar com.dalet.log4shell.AnyDirPatcher "C:\Program Files (x86)\AmberFin"
Patching jar: C:\Program Files (x86)\AmberFin\AmberFinAnalytics\AnalyticsService\WEB-INF\lib\log4j-core-2.8.2.jar
Patched jar: C:\Program Files (x86)\AmberFin\AmberFinAnalytics\AnalyticsService\WEB-INF\lib\log4j-core-2.8.2.jar
can't open C:\Program Files (x86)\AmberFin\iCR\JRE_x64\lib\tz mappings.
Patching jar: C:\Program Files (x86)\AmberFin\AmberFinDark\ProfileEditor\WEB-INF\lib\log4j-core-2.10.0.jar
Patched jar: C:\Program Files (x86)\AmberFin\AmberFinDark\ProfileEditor\WEB-INF\lib\log4j-core-2.10.0.jar
Patching jar: C:\Program Files (x86)\AmberFin\AmberFinWorkflow\WorkflowEngineService\WEB-INF\lib\log4j-core-2.11.1.jar
Patched jar: C:\Program Files (x86)\AmberFin\AmberFinWorkflow\WorkflowEngineService\WEB-INF\lib\log4j-core-2.11.1.jar
Patching jar: C:\Program Files (x86)\AmberFin\AmberFinWorkflow\WorkflowManagerService\WEB-INF\lib\log4j-core-2.11.1.jar
Patched jar: C:\Program Files (x86)\AmberFin\AmberFinWorkflow\WorkflowManagerService\WEB-INF\lib\log4j-core-2.11.1.jar

C:\Users\ingest-test.DALET\Desktop\LogPatcher>PAUSE
Press any key to continue . . .
```

5. Repeat this process for all AmberFin installed servers.