AEMO Data Interchange applications patch

Audience

All participants using the AEMO Data Interchange software, regardless of the version you are running.

Issue

A critical zero-day vulnerability has been identified by Apache Software Foundation in the popular Java logging library (log4j version 2) that can allow remote code execution of affected systems. This vulnerability is impacting servers worldwide.

The AEMO Data Interchange software uses v2.8.1 of the Log4j library, and this specific version has been identified as impacted by this vulnerability.

This document contains important instructions of actions that can be taken by participants on existing Data Interchange software installations to close the vulnerability

Solution

AEMO is proposing a 2-stage approach in response to this advised threat.

Stage 1 - Containment

AEMO will temporarily remove access to download the installation media of the Data Interchange applications on both the EMMS Preproduction participant server and via the AEMO website. This action is necessary to prevent new installations containing the vulnerability being created.

In accordance with advice issued by the Log4J2 community, Participants are recommended to take the following actions for each pdrBatcher, pdrLoader and pdrMonitor installation:

1. Navigate to the Lib installation folder
2. Confirm the version of the Log4J2 library. The current production releases of AEMO Data interchange software all ship with:

   log4j-core-2.8.1.jar

3. Make a backup of the log4j-core-2*.jar, but ensure that this is outside of the Lib installation folder. The purpose of this backup is to create a recovery point.

4. Remove the JndiLookup class from the Log4J2 core jar file

For windows type environments:

Step 1 – Create file log4j2_vulnerability_patch.ps1 in Lib folder with the following contents. Ensure that the specification of $zipFile matches the log4j-core-*.jar file in your installation and adjust as required

```
########################################################################
#
#   Name:         log4j2_vulnerability_patch.ps1
#   Purpose:      Script which removes the JndiLookup class from a Log4J2
installation
#                       Required to remediate remote code execution vulnerability
(CVE-2021-44228)
#                       affecting Log4j versions 2.0-beta9 to 2.14.1
#   Author:             AEMO
#   Date:         13th December 2021
#   Version:      1.0
#   Modifications:
#
########################################################################

[Reflection.Assembly]::LoadWithPartialName('System.IO.Compression')

$zipfile = 'log4j-core-2.8.1.jar'
$files   = 'JndiLookup.class'

$stream = New-Object IO.FileStream($zipfile, [IO.FileMode]::Open)
$mode   = [IO.Compression.ZipArchiveMode]::Update
$zip    = New-Object IO.Compression.ZipArchive($stream, $mode)

($zip.Entries | ? { $files -contains $_.Name }) | % { $_.Delete() }

$zip.Dispose()
$stream.Close()
$stream.Dispose()
```

Step 2 – Run the above PowerShell script from the command prompt:

```
powershell -executionpolicy bypass -file log4j2_vulnerability_patch.ps1
```

For Linux type environments:

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

Manually:

```
Open log4j-core-2.8.1.jar with your favourite zip compression tool and remove
file org/apache/logging/log4j/core/lookup/JndiLookup.class
```

5. To validate the fix has been effective inspect the log4j-core-2.8.1.jar file with any zip capable tool and ensure that the JndiLookup.class has been removed. It is also important not to keep a backup copy of the log4j-core-2.8.1.jar file in the Lib folder with a .JAR extension otherwise the AEMO Data Interchange application may use the backup and not the modified version of the library.

6. Restart the application running out of this installation directory. It is critical that you take this action or the remediation may not be effective.

7. Validate that the application is logging as expected. When confirmed the backup of log4j-core-2.8.1.jar created in Step 3 should be removed to ensure it does not unintentionally get re-instated to the application installation directory.

Stage 2 - Restoration

AEMO will provide updated builds for all Data Interchange applications such that a clean full install will not contain the Log4J2 vulnerability. Once new builds have been verified, they will be made available across the various publication points and access to these publication points restored. AEMO will advise the timing of this in a future notice to participants.

For any participant who requires access to the installation media of the Data Interchange applications, please contact the AEMO Support hub and we will arrange to provide this to you along with this instruction to ensure that any new installations are secure.

Participant action required

Regardless of the Data Interchange applications you have installed, AEMO strongly recommends participants to apply this patch update to ensure the security of your Data Interchange installations.