Lumada Data Catalog

CVE-2021-45105 – log4j vulnerability hotfix ReadMe

Contents

About this Document

This document provides information about issues addressed as vulnerability hotfix for Lumada Data Catalog (LDC) version 6.1.1, 6.0.1, and 2019.3.

Intended audience

This document is intended for customers and Hitachi Vantara partners who license and use Lumada Data Catalog.

Getting help

To request technical support, you may log on to the Support Portal and or open a Support ticket by sending an email to support.pentaho@hitachivantara.com.

Accessing product downloads

Product Downloads, Documentation, Technical Notes, a Knowledge Base, and Tutorials are available on the Waterline Data Customer Portal. Log on and select Product Downloads, Documentation, and Tutorials.

About this hotfix

This vulnerability hotfix addresses the mitigation and resolution for the vulnerability identified on Apache log4j component that is used in Lumada Data Catalog release 6.1.1, 6.0.1, and 2019.3. This hotfix addresses the previously detected vulnerabilities for Apache log4j including CVE-2021-44228, CVE-2021-45046, CVE-2021-45105. Click the links for details on these vulnerabilities.

These resolution steps are described in the “Applying the hotfix” section.

Fixed Issues

1. IN-21410: Update log4j version to log4j-2.17.0 to address CVE-2021-45105. This also addresses CVE-2021-44228 and CVE-2021-45046, and version updates for Apache Atlas connector where configured.

Applying the hotfix

This fix is to be applied on version 6.1.1, 6.0.1 or 2019.3 at any patch and/or hotfix level

1. Stop all Data Catalog components, if already running. Be sure to follow the specified sequence below.

```
<Agent Dir>$ bin/agent stop

<Metadata-Server Dir>$ bin/metadata-server stop

<App-Server Dir>$ bin/app-server stop
```

   The agent stop command must be executed on all machines where an Agent is installed.

2. Download the vulnerability hotfix for Lumada Data Catalog 6.1.1, 6.0.1 and 2019.3 and note the download location `<download location>`. Note that there is one tar file: `cve-2021-45105-log4j-HF.tar`

3. Backup the lib directories on all three LDC components as follows:

```
<Agent Dir>$ cp lib <Backup-Location>/agent-lib-bkup<current-date>

<Metadata-Server Dir>$ cp lib <Backup-Location>/metadata-server-lib-
bkup<current-date>

<App-Server Dir>$ cp lib <Backup-Location>/app-server-lib-bkup<current-date>
```

4. Extract the tar file in the `<download location>` and run the extracted upgrade script as the service user with the relevant permissions as follows:

```
<download-location>$ tar -xvf cve-2021-45105-log4j-HF.tar
```

   a. Run the Upgrade script for the **Application Server component**

```
<download-location>$ ./upgrade.sh

  ***************************
  Catalog ZeroDay Log4j Fixer
  ***************************
  Location of component: (Default: /opt/ldc/app-server) /opt/ldc/app-server
```

   NOTE: The script automatically replaces the vulnerable versions of log4j files in the Application Server directory with the recommended version 2.17.0

b. Rename the backup directory as `app-server-bkup<current-date>`

```
<download-location>$ mv backup app-server-backup<current-date>
```

c. Run the Upgrade script for the **Metadata Server component**

```
<download-location>$ ./upgrade.sh

  ***************************
  Catalog ZeroDay Log4j Fixer
  ***************************
  Location of component: (Default: /opt/ldc/app-server) /opt/ldc/metadata-
  server
```

NOTE: The script automatically replaces the vulnerable versions of log4j files in the Metadata Server directory with the recommended version 2.17.0

d. Rename the backup directory as `metadata-server-bkup<current-date>`

```
<download-location>$ mv backup metadata-server-backup<current-date>
```

e. Run the Upgrade script for the **Agent component**

```
<download-location>$ ./upgrade.sh

  ***************************
  Catalog ZeroDay Log4j Fixer
  ***************************
  Location of component: (Default: /opt/ldc/app-server) /opt/ldc/agent
```

NOTE: The script automatically replaces the vulnerable versions of log4j files in the Agent directory with the recommended version 2.17.0

f. Rename the backup directory as `agent-bkup<current-date>`

```
<download-location>$ mv backup agent-backup<current-date>
```

The upgrade script for the agent must be executed on all machines where an Agent is installed.

g. Run the Upgrade script for the **Atlas connector**

```
<download-location>$ ./upgrade.sh

  ***************************
  Catalog ZeroDay Log4j Fixer
  ***************************
  Location of component: (Default:/opt/ldc/app-server)
  /opt/ldc/agent/adapters/atlas/
```

NOTE: The script automatically replaces the vulnerable versions of log4j files in the Atlas connector directory with the recommended version 2.17.0

h. Rename the backup directory as `atlas-connector-bkup<current-date>`

```
<download-location>$ mv backup app-server-backup<current-date>
```

5. Start all Data Catalog services.

   ```
   <App-Server Dir>$ bin/app-server start
   <Metadata-Server Dir>$ bin/metadata-server start
   <Agent Dir>$ bin/agent start
   ```

   The agent start command should be executed on all machines where an Agent is installed.

6. Check if the metadata server is connected.
   If metadata server is not connected, re-initialize the metadata server by using the `--init` command with the metadata-server script on the metadata-server node.

   You can obtain the `--endpoint`, `--client-id`, `--metadata-rest-server-token, --public-host,` and `--port` details from the installation string for the Metadata Server under **Manage -> Tokens -> <metadata-rest-server> -> Re-install metadata-rest-server**.

   ```
   <Metadata-Server Dir>$ bin/metadata-server init --endpoint <endpoint> --
   client-id metadata-rest-server --token <token> --public-host <public host> --
   port <port>
   ```

7. Check if all agents are connected.
   If any agent is not connected, re-register that agent by using the `--register` command with the agent script on the agent node.

   You can obtain the `--endpoint`, `--agent-id`, `--agent-token`, and `--cert-fingerprint` details from the registration string for the agent under **Manage -> Agents -> <Agent name> -> Register Agent**.

   ```
   <Agent Dir>$ bin/agent register --endpoint <endpoint> --agent-id <agent-id> -
   -agent-token <token> --cert-fingerprint <ssl SHA256 fingerprint of secure
   endpoint>
   ```