1.x - H2 database CVE mitigation

Introduction

A critical vulnerability has been discovered in the third-party tool **h2 database** (all releases prior to **2.0.206**) used by both the Console front-end package and the Node back-end package:

- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42392**

The h2 database is used by **all 1.x releases of Console/Node** (2.x releases do not use the h2 database) and therefore **all 1.x releases are impacted** by this CVE. See also **https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/**.

Updates to Console/Node packages

CAST does NOT intend to provide a new release of Console 1.x that includes a new release of h2 database that includes the fix for this CVE. This is because the releases of h2 database that include the CVE fix are not compatible with the release of h2 database that CAST uses, and therefore a full database migration would be necessary with all the risk associated with it.

What you can do to prevent the vulnerability from being exploited

To mitigate the risk posed by this CVE, you should perform the following actions.

Disable and prevent access to the h2 database UI console

First locate the following property files in your deployment:

```
Console:
%PROGRAMDATA%\CAST\AipConsole\AipConsole\aipConsole.properties

Node (if you have more than one Node, all Nodes must be taken into account):
%PROGRAMDATA%\CAST\AipConsole\AipNode\aip-node-app.properties
```

In these property files, locate the following section:

```
# ============
# Datasource
# ------------
spring.datasource.url=jdbc:h2:file:C:/Program Data/CAST/AipConsole/AipNode/db/aip_node_db;AUTO_SERVER=TRUE
spring.datasource.username=sa
spring.datasource.password=
spring.datasource.driver-class-name=org.h2.Driver
spring.jpa.database-platform=org.hibernate.dialect.H2Dialect
spring.jpa.hibernate.ddl-auto=none
spring.h2.console.enabled=false
spring.h2.console.path=/h2
```

Now ensure that the following line is set to **false** - this should already be the case since this property is set to false out of the box. This property (when set to false) disables the h2 database web based console which is the most severe attack vector for this CVE:

```
spring.h2.console.enabled=false
```

Then **add a new line** in the section as follows. This property ensures that the h2 database web based console (if enabled) can only be accessed by localhost (not other devices on the LAN):

```
spring.h2.console.settings.web-allow-others=false
```

Finally, restart the following to ensure the change is taken into account:

- Console front-end
- All Node back-ends

If you need to have access to the h2 database UI console, you should enable authentication on it by adding the property `spring.h2.console.settings.web-admin-password` in the Console/Node property files and setting it to a value you want to use to protect the h2 Console.

Other mitigations

Other mitigation tactics include **updating the JRE/JDK** installed on the host servers for use by Console and all Nodes, to include a check called `trustURLCodebase` that prevents loading remote codebases from JNDI. This update has been added in:

- Java 8 update 191
- Java 11.0.1

The `trustURLCodebase` property should be set to **false** and you can do this by adding `-DtrustURLCodebase=false` to the Console and Node bat files used to launch the services:

```
Console:
start "AIP Console" /D "%CONSOLE_FOLDER%" java -jar -Xmx2048m -Xms1024m "bin/aip-console-app.jar" -
DtrustURLCodebase=false

Node:
java -jar -Xmx2048m -Xms1024m "bin/aip-node-app.jar" -DtrustURLCodebase=false
```


Note, however, that this mitigation is **not possible** if you are using **Microsoft Windows services** to run Console/Nodes.