zellis

PROIV Technology Mitigation for Log4J Security Vulnerability CVE-2021-44228

zellis.com

Table of Contents

Document Control

Document Information

	Information
Document Id	PROIV Log4J Mitigation
Document Owner	Zellis
Issue Date	13/12/2021
Last Saved Date	13/12/2021
File Name	PROIV Log4J Mitigation

Document History

Version	Issue Date	Changes
1.0	13/12/2021	Draft

Introduction

This document details the configuration steps required to mitigate Apache Log4j2 vulnerability - CVE-2021-44228 in an installation of PROIV version 9.4 or above or PROIV version 10. It is not applicable to earlier releases of version 9 (9.3 or earlier) or any releases of version 8 or version 7.

Reconfiguring PROIV Version 9 / 10 Virtual Machine

Re-Configuring the PROIV Virtual Machine via the Dashboard

Perform the following steps to apply the mitigation to a PROIV Version 9 / 10 virtual machines configuration.

1. Navigate to the configuration profile you wish to apply the mitigation to.
2. Select the **Virtual Machine / Settings**
3. Scroll down to the **Server Side Objects** section
4. Update the value in the **Options** setting to include **-Dlog4j2.formatMsgNoLookups=true**
5. Scroll to the bottom of the configuration and press Submit to persist the configuration

You now need to redeploy the Virtual Machine configuration, navigate to your deployment and press the slider next to **Virtual Machine** to redeploy it. Note you may be asked if you want to redeploy Application Connector and Client Connector. This configuration change does not require them to be redeployed. However once have redeployed the Virtual Machine it is recommended that you restart the Application Connector and Client Connector services.

Re-Configuring the PROIV Virtual Machine by editing VM Configuration file

Open the configuration file (usually with the extension .properties) in your favourite text editor and locate the line which starts:

```
proiv.virtualMachine.java.options=
```

This configuration should be changed to

```
proiv.virtualMachine.java.options=-Dlog4j2.formatMsgNoLookups=true
```

Once the file is saved then all new Virtual Machine processes that are started will use the new setting. If you are using the Version 10 Task Server on UNIX then you should also restart that process.

It is important to note that this change is not persisted in the dashboard configuration, subsequent redeployments will overwrite it unless it is updated via the dashboard.

Re-Configure the PROIV Web Applications

In order to apply the mitigation to the PROIV Java services, it is necessary to update the configuration file named `wrapper.conf`.

The configuration file can be found in the following locations in a PROIV installation (this is applicable to both Windows and UNIX installations).

```
LicenceServices/conf/wrapper.conf
SystemServices/conf/wrapper.conf
ApplicationServices/conf/wrapper.conf
ClientServices/conf/wrapper.conf
AnalyticServices/conf/wrapper.conf
```

In order to apply the mitigation, you need to stop all the services and edit each file in turn following the guidance below and then restart all the services as you would do normally.

Locate the section of the file containing lines `wrapper.java.additional.x`

The snip of configuration lines below is from an installation of PROIV Version 10 on Windows where PROIV is installed in `c:\prov10`. It is

```
# Java Additional Parameters
wrapper.java.additional.1=-Djetty.home="c:\prov10\_jetty"
wrapper.java.additional.2=-Djetty.base="c:\prov10\SystemServices"
wrapper.java.additional.3=-DSTOP.PORT=-1
wrapper.java.additional.4=-Dapp.home="c:\prov10\SystemServices"
wrapper.java.additional.5=-Dderby.system.home="c:\prov10\SystemServices\_proiv_system_db"
wrapper.java.additional.6=-Djava.io.tmpdir="c:\prov10\SystemServices\temp"
```

Add a new additional parameter, choose the next number in the list, in the case above

```
wrapper.java.additional.7=-Dlog4j2.formatMsgNoLookups=true
```

Note that each of the configuration files may have a different number of additional parameters so do not cut and paste it is important to ensure that the numbers are contiguous.

zellis