Instructions provided by Fortinet Engineering - December 11, 2021 5:39:37 PM

Mitigating CVE-2021-44228

FortiSIEM uses Apache log4j version 2.14 for logging purposes, and hence is vulnerable to the recently discovered Remote Code Execution vulnerability (CVE-2021-44228).

This note specifies the steps needed to mitigate this vulnerability without upgrading Apache log4j to version 2.15.

On the Supervisor Node:

Login to the Supervisor node via SSH as root and perform the following steps.

Step 1 Backup current App Server configuration:

Run these commands

```
# cp -a /opt/glassfish/domains/domain1/config/domain.xml
/opt/glassfish/domains/domain1/config/domain.xml.bak
# cp -a /opt/phoenix/config/log4j.properties /opt/phoenix/config/log4j.properties.bak
```

Step 2 (Optional) Backup current log4j configuration for use by Java Query Server configuration in Elasticsearch based deployments

Run this command

```
# cp -a /opt/phoenix/config/javaQueryServer/log4j.properties
/opt/phoenix/config/javaQueryServer/log4j.properties.bak
```

Step 3 Modify log4j configuration for use by App Server

The file is located in `/opt/phoenix/config/log4j.properties`

Step 3.1 Replace these 2 lines in the file

```
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m%n
```

With these two lines

```
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m{nolookups}%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m{nolookups}%n
```

Step 3.2 Add this line at the end of the file

```
log4j2.formatMsgNoLookups=True
```

Instructions provided by Fortinet Engineering - December 11, 2021 5:39:37 PM

Step 4 Modify domain.xml file for use by App Server

The file is located in */opt/glassfish/domains/domain1/config/domain.xml*

Add this line in in the java-config block:

```
<jvm-options>-Dlog4j2.formatMsgNoLookups=true</jvm-options>
```

After modification, the java-config block in the file will look like this:

```
<java-config classpath-suffix="" debug-options="-Xdebug -
Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=9009" system-classpath="">
   <jvm-options>-XX:MaxPermSize=384m</jvm-options>
    …
   <jvm-options>-Dcom.sun.enterprise.server.logging.max_history_files=20</jvm-options>
   <jvm-options>-Dlog4j2.formatMsgNoLookups=true</jvm-options>
 </java-config>
```

Step 6 (Optional) Modify log4j configuration for use by Java Query Server module in Elasticsearch based deployments

If you are not running Elasticsearch, then skip this step.

The file is located in `/opt/phoenix/config/javaQueryServer/log4j.properties`

Replace these 3 lines

```
log4j.appender.stdout.layout.ConversionPattern=%5p [%t] (%F:%L) - %m%n
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m%n
```

With these 3 lines

```
log4j.appender.stdout.layout.ConversionPattern=%5p [%t] (%F:%L) - %m{nolookups}%n
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m{nolookups}%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m{nolookups}%n
```

Step 7 Restart App Server

```
Run this command: "killall -9 java"
```

On each Worker and Collector Node:

Login to the Worker node via SSH as root and perform the following steps

Step 1 Backup current log4j configuration:

Run this command:

```
# cp -a /opt/phoenix/config/log4j.properties /opt/phoenix/config/log4j.properties.bak
```

Step 2 Modify log4j configuration:

Instructions provided by Fortinet Engineering - December 11, 2021 5:39:37 PM

The file is located in `/opt/phoenix/config/log4j.properties`

Replace these 2 lines in the file

```
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m%n
```

With these two lines:

```
log4j.appender.R.layout.ConversionPattern=%d %p [%t] %c - %m{nolookups}%n
log4j.appender.SYSLOG.layout.ConversionPattern=%d{MMM dd HH:mm:ss} %m{nolookups}%n
```

Step 3 Restart Java

Run this command: “killall -9 java”