Kepler - Bug #6928

Check Kepler for the Apache commons deserialization problems, consider removing the commons-collections-3.2.1 jar file

01/04/2016 01:21 PM - Christopher Brooks

Status:	Resolved	**Start date:**	01/04/2016
Priority:	Normal	**Due date:**	
Assignee:	Daniel Crawl	**% Done:**	0%
Category:	build system	**Estimated time:**	0.00 hour
Target version:	2.6.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

I recently had a Windows machine that was successfully attacked because it was running an old version of Jenkins that was susceptible to an attack via Apache Commons Java deserialization. The email from campus stated:

> "The snort alarms concern an apparent remote attack against a "serious vulnerability in Apache Commons, a library that contains a widely used set of Java components maintained by the Apache Software Foundation, puts thousands of Java applications and servers at risk of remote code execution attacks. The library is used by default in multiple Java application servers and other products including Oracle WebLogic, IBM WebSphere, JBoss, Jenkins and OpenNMS."
>
> "Please see"
>
> http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/
>
> http://www.oracle.com/technetwork/topics/security/alert-cve-2015-4852-2763333.html
>
> https://blogs.apache.org/foundation/entry/apache_commons_statement_to_widespread

It looks like Kepler includes the library in question:

```
bash-3.2$ find . -name "*.jar" | xargs grep -Rl InvokerTransformer
./configuration-manager/lib/jar/commons-collections-3.2.1.jar
```

commons-collections-3.2.1.jar contains classes in packages starting with org.apache.commons.collections

However, I believe that the Kepler *.java files are not directly using those classes, below are classes in org.apache.commons that are imported. Note that we are not importing classes from org.apache.commons.collections:

```
bash-3.2$ find . -name "*.java" | xargs grep org.apache.commons | grep import | tr -d '\r' | awk '
{print $NF}' | sort | uniq -c | sort -nr
 235 org.apache.commons.logging.LogFactory;
 235 org.apache.commons.logging.Log;
   3 org.apache.commons.io.IOUtils;
   3 org.apache.commons.configuration.XMLConfiguration;
   2 org.apache.commons.net.ftp.FTP;
   2 org.apache.commons.lang.StringEscapeUtils;
   2 org.apache.commons.io.FileUtils;
   2 org.apache.commons.httpclient.methods.multipart.StringPart;
   2 org.apache.commons.httpclient.methods.multipart.Part;
   2 org.apache.commons.httpclient.methods.multipart.FilePart;
   2 org.apache.commons.httpclient.methods.MultipartPostMethod;
   2 org.apache.commons.httpclient.methods.GetMethod;
   2 org.apache.commons.httpclient.HttpException;
   2 org.apache.commons.httpclient.HttpClient;
```

```
   2 org.apache.commons.configuration.ConfigurationException;
   1 org.apache.commons.lang.time.DateUtils;
   1 org.apache.commons.lang.exception.ExceptionUtils;
   1 org.apache.commons.io.FilenameUtils;
   1 org.apache.commons.configuration.tree.ConfigurationNode;
   1 org.apache.commons.configuration.PropertiesConfiguration;
   1 org.apache.commons.configuration.HierarchicalConfiguration;
bash-3.2$
```

However, there could be dependencies between jar files used by Kepler and commons-collections-3.2.1.jar.

https://www.kb.cert.org/vuls/id/576313 suggests upgrading to Apache Commons Collections version 3.2.2

However, perhaps we can remove this class?

The log is below:

```
bash-3.2$ svn log ./configuration-manager/lib/jar/commons-collections-3.2.1.jar
------------------------------------------------------------------------
r24000 | berkley | 2010-04-27 17:12:36 -0700 (Tue, 27 Apr 2010) | 1 line

changing keywords and eol-style on the repository
------------------------------------------------------------------------
r20925 | berkley | 2009-10-07 15:06:24 -0700 (Wed, 07 Oct 2009) | 1 line

writing tests to show the capabilities of commons and yaml and to compare them
------------------------------------------------------------------------
bash-3.2$
```

History

#1 - 01/04/2016 01:52 PM - Daniel Crawl

- Status changed from New to Resolved

- Target version set to 2.6.0

Thanks for the notice about the vulnerability, Christopher.

I tried removing the jar, but got an exception from org.kepler.configuration.CommonsConfigurationReader when Kepler starts, so I updated commons-collections to 3.2.2.

#2 - 01/04/2016 02:05 PM - Christopher Brooks

Thanks for the quick turn around on this. I submitted it as a bug so that there was a more permanent record of the action taken to solve this.