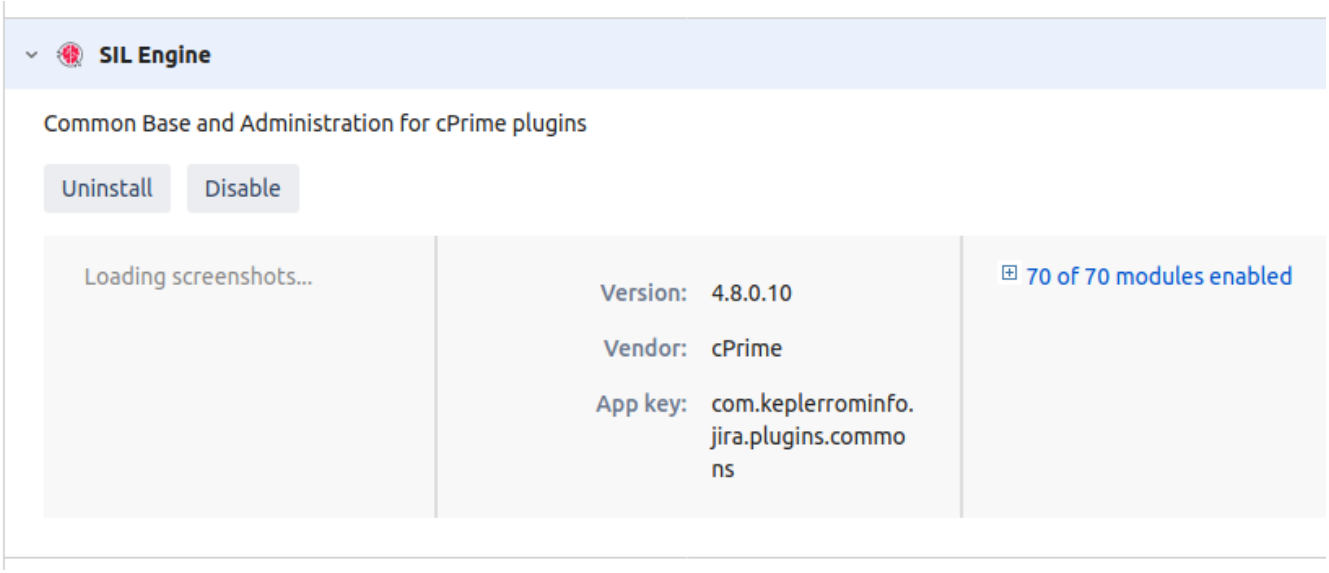
Jira attempting to create ksil_userpicker.jsp ??

This page constitutes random notes from my work day as an Atlassian product consultant, put up in the vague hope they might benefit others. Expect rambling, reference to unsolved problems, and plenty of stacktraces. **Check the date** as any information given is likely to be stale.

A suprising log I noticed on JIRA startup today:

```
    2020-07-11 14:18:29,465+1000 JIRA-Bootstrap ERROR      [c.k.j.p.keplercf.admin.KCFLauncher] Cannot copy the
JSP. Error was:java.io.FileNotFoundException: /opt/atlassian/redradish_jira/8.10.0/atlassian-jira/secure/popups
/ksil_userpicker.jsp (Permission denied)
java.io.FileNotFoundException: /opt/atlassian/redradish_jira/8.10.0/atlassian-jira/secure/popups
/ksil_userpicker.jsp (Permission denied)
        at java.base/java.io.FileOutputStream.open0(Native Method)
        at java.base/java.io.FileOutputStream.open(FileOutputStream.java:298)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:237)
        at java.base/java.io.FileOutputStream.<init>(FileOutputStream.java:187)
        at com.keplerrominfo.jira.plugins.keplercf.admin.KCFLauncher.copyJSPFile(KCFLauncher.java:346)
        at com.keplerrominfo.jira.plugins.keplercf.admin.KCFLauncher.launch(KCFLauncher.java:188)
        at com.keplerrominfo.refapp.launcher.AbstractDependentPluginLauncher.tryToLaunch
(AbstractDependentPluginLauncher.java:139)
        at com.keplerrominfo.refapp.launcher.AbstractDependentPluginLauncher.handleEvent
(AbstractDependentPluginLauncher.java:85)
        at com.keplerrominfo.jira.plugins.keplercf.admin.KCFLauncher.onPluginEvent(KCFLauncher.java:215)
        at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
        at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
43)
        at java.base/java.lang.reflect.Method.invoke(Method.java:566)
        at com.atlassian.event.internal.SingleParameterMethodListenerInvoker.invoke
(SingleParameterMethodListenerInvoker.java:42)
        at com.atlassian.event.internal.AsynchronousAbleEventDispatcher.lambda$null$0
(AsynchronousAbleEventDispatcher.java:37)
        at com.atlassian.event.internal.AsynchronousAbleEventDispatcher.dispatch
(AsynchronousAbleEventDispatcher.java:85)
        at com.atlassian.event.internal.LockFreeEventPublisher$Publisher.dispatch(LockFreeEventPublisher.java:
220)
        at com.atlassian.event.internal.LockFreeEventPublisher.publish(LockFreeEventPublisher.java:96)
...
2020-07-11 12:26:36,465+1000 UpmAsynchronousTaskManager:thread-2 ERROR jturner 736x198x1 1uhj4pl 127.0.0.1 /rest
/plugins/1.0/updates/all [c.k.j.p.keplercf.admin.KCFLauncher] You must manually copy the ksil_userpicker.jsp
file into the correct directory (read the manual). Destination path: JIRA-HOME/atlassian-jira/secure/popups
/ksil_userpicker.jsp
```

It appears this is caused by the SIL Engine plugin:



SIL Engine is attempting to copy a JSP to JIRA's app directory, and failing due to permissions.

SIL Engine is a "library plugin", a dependency of other CPrime plugins, which I had experimented with in the past (Power Custom Fields, I think). The problem with "library plugins" is that they hang around even after the last plugin that used them is uninstalled. Thus; SIL Engine on my system.

Digression: Permissions in your /opt/atlassian/jira directory

The attempted copy failed ('Permission Denied'), and rightly so. JIRA (and any webapp) should absolutely not be allowed to write to its own installation directory. Back in 2009 I had not learned this. I was a volunteer administrator of https://jira.apache.org, and left the app directory writable, which contributed to the server being hacked:

What Happened?

On April 5th, the attackers via a compromised Slicehost server opened a new issue, INFRA-2591. This issue contained the following text:

> ive got this error while browsing some projects in jira http://tinyurl.com/XXXXXXXXX [obscured]

Tinyurl is a URL redirection and shortening tool. This specific URL redirected back to the Apache instance of JIRA, at a special URL containing a cross site scripting (XSS) attack. The attack was crafted to steal the session cookie from the user logged-in to JIRA. When this issue was opened against the Infrastructure team, several of our administators clicked on the link. This compromised their sessions, including their JIRA administrator rights.

At the same time as the XSS attack, the attackers started a brute force attack against the JIRA login.jsp, attempting hundreds of thousands of password combinations.

On April 6th, one of these methods was successful. Having gained administrator privileges on a JIRA account, the attackers used this account to disable notifications for a project, and to change the path used to upload attachments. The path they chose was configured to run JSP files, and was writable by the JIRA user. They then created several new issues and uploaded attachments to them. One of these attachments was a JSP file that was used to browse and copy the filesystem. The attackers used this access to create copies of many users' home directories and various files. They also uploaded other JSP files that gave them backdoor access to the system using the account that JIRA runs under.

By the morning of April 9th, the attackers had installed a JAR file that would collect all passwords on login and save them.

Countless PHP hacks have been enabled to not following this rule, due to apps like Wordpress encouraging the anti-pattern of allowing the app to upgrade itself.

But what about ksil_userpicker.jsp?

There is nothing on the web about ksil_userpicker.jsp, so I contacted CPrime. Developer Radu Dumitriu replied:

> *That file was necessary because, at the time, Jira didn't have the ability to let us create a user picker panel (3.x). That's the solution we came with, so obviously it remained unchanged. We will change that when we'll publish a major version of the addon (hopefully).*

> *So the answer to both your questions is 'history' blocked URL*

So it looks innocuous. Still, I think it best to ignore the error until usage actually demands this JSP's presence. If, like for me, SIL Engine is a relic, you would be best off uninstalling it.