**SUMMARY**

A concurrency bug in Apache Tomcat5 5.0.28.

**DETAILS**

Some details can also be found at: https://bz.apache.org/bugzilla/show\_bug.cgi?id=33743

This bug is due to a data race.

WebAppClassLoader may fail if concurrent threads try to load a not-yet-loaded class.

Scenario:

two threads enter loadClass(name, resolve) (line 1214) concurrently. none of them finds a loaded class, so both enter findClass (827) and findClassInternal (1559).

Now one thread goes ahead, finds the resource and defines the class.

Consequently, it sets entry.binaryContent to null (1633). Thread 2 now checks binaryContent for null (1572) and throws a ClassNotFoundException.

In the field, this error occurs, if you start Tomcat and load a number of different jsps concurrently that all use the same tag class.

I also have a standalone testcase where I made WCL#addRepository(String,File) public.

As it seems, #loadClass(String, boolean) (1211) should be synchronized, as in the superclasses.

|  |  |
| --- | --- |
| Thread1 (WebappClassLoader.java) | Thread2 (WebappClassLoader.java) |
| protected Class findClassInternal(String name)  throws ClassNotFoundException {  …  if ((entry == null) || (entry.binaryContent == null))  throw new ClassNotFoundException(name);  ..  if (entry.loadedClass == null) {  synchronized (this) {  if (entry.loadedClass == null) {  clazz = defineClass(name, entry.binaryContent, 0,  entry.binaryContent.length,  codeSource);  entry.loadedClass = clazz;  entry.binaryContent = null;  entry.source = null;  entry.codeBase = null;  entry.manifest = null;  entry.certificates = null;  } else {  clazz = entry.loadedClass;  }  }  } else {  clazz = entry.loadedClass;  } | protected Class findClassInternal(String name)  throws ClassNotFoundException {  …  if ((entry == null) || (entry.binaryContent == null))  throw new ClassNotFoundException(name);  ..  if (entry.loadedClass == null) {  synchronized (this) {  if (entry.loadedClass == null) {  clazz = defineClass(name, entry.binaryContent, 0,  entry.binaryContent.length,  codeSource);  entry.loadedClass = clazz;  entry.binaryContent = null;  entry.source = null;  entry.codeBase = null;  entry.manifest = null;  entry.certificates = null;  } else {  clazz = entry.loadedClass;  }  }  } else {  clazz = entry.loadedClass;  } |
| 0-lock | 1-lock |