The Good, The Bad and The Ugly

Mark Thomas, Staff Engineer

Agenda

- Introductions
- The Good
- The Bad
- The Ugly
- Reflections
- Questions

Introductions

Introductions

- **Mark Thomas**
- **Apache Tomcat committer (markt)**
- **Other ASF**
  - Infrastructure team
  - Security
  - Commons
  - Member
- **Staff Engineer at VMware**
  - Tomcat
  - Security
  - tc Server
  - support

The Good

How things are meant to work

The Good

- **Applies to most Tomcat vulnerability reports**
- **Roughly between 5 and 20 valid vulnerability reports a year**
- **Usually apply to multiple versions**
- **Tomcat 7 severities**
  - Critical None
  - Important 14
  - Moderate 2
  - Low 7
- **Usually months from disclosure to announcement**
  - Due to slow release cycle for older versions

The Good: CVE-2012-2733

- HTTP header size limits not enforced for the HTTP NIO connector
- 04 Jun: OP reports issue
- 05 Jun: Forwarded to Tomcat security team
- 05 Jun: Acknowledgement sent to the OP
- 07 Jun: Test case written to reproduce the issue
- 10 Jun: Proposed patch
- 14 Jun: Issue confirmed to OP
- 14 Jun: CVE requested and received
- 19 Jun: 7.0.28 released
- 19 Oct: 6.0.36 released
- 19 Oct: Draft announcement sent to OP
- 05 Nov: Announcement issued

The Bad

The many, many ways I managed to make mistakes

The Bad

- **CVE-2012-4431: coding error**
  - CSRF prevention filter bypass
  - The CSRF prevention filter could be bypassed if a request was made to a protected resource without a session identifier present in the request
- **CVE-2012-3439: incorrectly rejecting a valid report**
  - DIGEST authentication weaknesses
  - The original report contained some inaccuracies
  - I incorrectly dismissed one of the report's concerns because I misread RFC2617
- **CVE-2012-4534: not spotting security implications**
  - Bug report of a client triggered infinite loop
  - DoS
  - Security implications not considered at the time

The Bad

- **CVE-2008-2938: co-ordination headaches**
  - Incorrect handling of invalid UTF-8 led to directory traversal
  - The root cause was a bug in the Java UTF-8 decoder
  - The OP did not realise what they had found
  - Sun did not accept it was a security vulnerability
  - Information started to leak out
  - Lots of vendors patched their application servers to work-around the problem
  - Once the JVMs were all fixed the correct information was published
- **CVE-2008-2938 (again): finger trouble**
  - I managed to send a draft vulnerability announcement to the users list

The Ugly

When you just want it all to stop…

The Ugly

- **CVE-2012-0022: Leaks, denials and dealing with the fall-out**
- **Java Hash collision issue**
  - Caused performance / DoS issues with lots of Java based applications
  - Tomcat affected via HTTP parameter parsing
  - Oracle did not treat it as a vulnerability
  - I'm still not sure if they should have or not
- **Names have be changed to protect the guilty**
  - The Tomcat project has dealt with many security co-ordination organisations
  - Usually they are well informed, very professional and a pleasure to deal with
  - OrgX replaces the name of the security coordination that passed this issue to us
- **Timeline is autumn 2011 to early 2012**

The Ugly

- **Oct 18: OrgX report problem with Geronimo**
- **Oct 18: OrgX report problem with unnamed ASF project**
- **Oct 19: ASF security team query target of second report**
- **Oct 19: OrgX identify Tomcat as target of second report**
- **Oct 19: OrgX passes on Metasploit PoC from OP**
- **Oct 19: OrgX informs ASF of proposed embargo date of 27 Dec**
- **Oct 25:**
  - Lots of issues in Tomcat's parameter parsing
  - Not related to hash collisions
  - With these issues fixed the metasploit PoC does not trigger a DoS
  - Tomcat team determines that a number of unrelated DoS issues have been found
  - Tomcat team opts to limit the number of parameters processed to as a precaution in case the hash collision vulnerability is an issue

The Ugly

- 27 Oct: Request and receive CVE-2011-4084 for DoS issues in Tomcat's parameter parsing
- 27 Oct: Inform OrgX of work to date and that reported vulnerability is not reproducible
- 27 Oct: Start committing patches for CVE-2011-4084
- 28 Oct: Make clear with OrgX that CVE-2011-4084 is for Tomcat's DoS issues, NOT for anything to do with hash collisions
- 28 Oct: I accidently commit my performance tests that I was using to debug the CVE-2011-4084 issues
- 29 Oct: OrgX asks permission to pass on patches for CVE-2011-4084 to other vendors. The Tomcat team does not reply.
- 31 Oct: Additional fixes for the parameter count limit identified
- 07 Nov: Complete patches in 7.0.x for CVE-2011-4084

The Ugly

- 10 Nov: Start patching 6.0.x for CVE-2011-4084
- 16 Dec: OrgX requests a CVE for the hash collision issue for Tomcat
- 16 Dec: The Tomcat team questions if the issue is valid
- 19 Dec: OP reports results and issues with maxParameterCount we can't reproduce
- 20 Dec: OP provides new Metasploit PoC
- 20 Dec: Inform OrgX that we can now reproduce the issue and that maxParameterCount is an effective mitigation
- 20 Dec: OrgX ask about what CVE will be used for what
- 20 Dec: ASF makes clear CVE-2011-4084 is for Tomcat's DoS issues only and that the hash collisions will require a different CVE
- 28 Dec: OP announces issue

The Ugly

- **28 Dec: ASF announces work-around (maxParameterCount)**
- **03 Jan: Information on CVE-2011-4084 leaks**
  - Discusses Tomcat generally being unable to handle large numbers of parameters
  - Also mentions hash table collisions
  - Looks like a merge of the two issues
- **03 Jan: Inform everyone with knowledge of CVE-2011-4084 that it has been leaked. Make it clear the ASF is not happy and ask for the person responsible to own up and apologise.**
- **03 Jan: Request and receive new CVE to replace CVE-2011-4084 (CVE-2012-0022)**

The Ugly

- 03 Jan: Discover that OrgX sent full details of CVE-2011-4084 to multiple vendors
- 03 Jan: Discover that OrgX announced hash collision vulnerability in Tomcat using CVE-2011-4084 leading several organisations to believe the previously issued information on CVE-2011-4084 was now public
- 03 Jan: OrgX denies being the source of the leak and states they believe no apology is necessary
- 03 Jan: Suggest to OrgX that they check again as we have a copy of the e-mail they denied sending

The Ugly

- **03 Jan: OrgX claims the information was only sent to the OPs**
- **03 Jan: ASF provides a quote of the email that leaked the information**
- **03 Jan: OrgX finally finds the e-mail and denies it is a leak**
- **03 Jan: ASF informs OrgX it disagrees with that view**
- **05 Jan: Various e-mails killing off CVE-2011-4084**
- **09 Jan: Complete patching 6.0.x for CVE-2011-4084**
  - There was a regression that wasn't fixed until just before the release
- **17 Jan: Announce CVE-2012-0022**

Reflections

Reflections

- **Time from report to announcement**
  - Driven by releases
  - Older versions have fewer releases
  - Unexpected release of old version (e.g. few weeks after last one) highly suggestive of a security issue
  - Balance issue severity against expected release schedule
- **Poor quality reports**
  - Have to take every report seriously
  - Consider each issue within a report separately
  - Even if the first 5 issues are nonsense, the 6th might be valid
- **Bug reports**
  - Any bug report might have security implications
  - Consider each bug with your security hat on

Reflections

- **E-mail**
  - Check your addressee lists before you send e-mail
  - Watch out for e-mail clients ‘helpfully’ displaying names rather than addresses
  - Then check your addressee lists again
- **Co-ordination authorities**
  - Can be very useful
  - Usually very professional
  - Rare problematic organisation / group / person
  - Don’t know there is a problem until it is too late
  - Used to default to trusting them
  - Now default to not trusting them until proven trustworthy
  - Generally, don’t pass on any new information you don’t have to

Questions