# JUDCon

JBoss Users & Developers Conference

2012:India

# JBoss security: penetration, protection and patching

David Jorm
djorm@redhat.com

# Contents

- The problem
- Background
- Historical vulnerabilities
- JBoss worm
- Security response for products
- The solution

# The Problem

# The problem

- JBoss is a major target, compromised JBoss servers are well documented
- We recently had a live worm that compromised thousands of servers
- Penetration testers focus on JBoss as a potential weak point
- JBoss products have coverage from SRT, JBoss projects are particularly exposed
- The main issues are insecure defaults and lack of patching/updating

# Background

# JBoss Projects

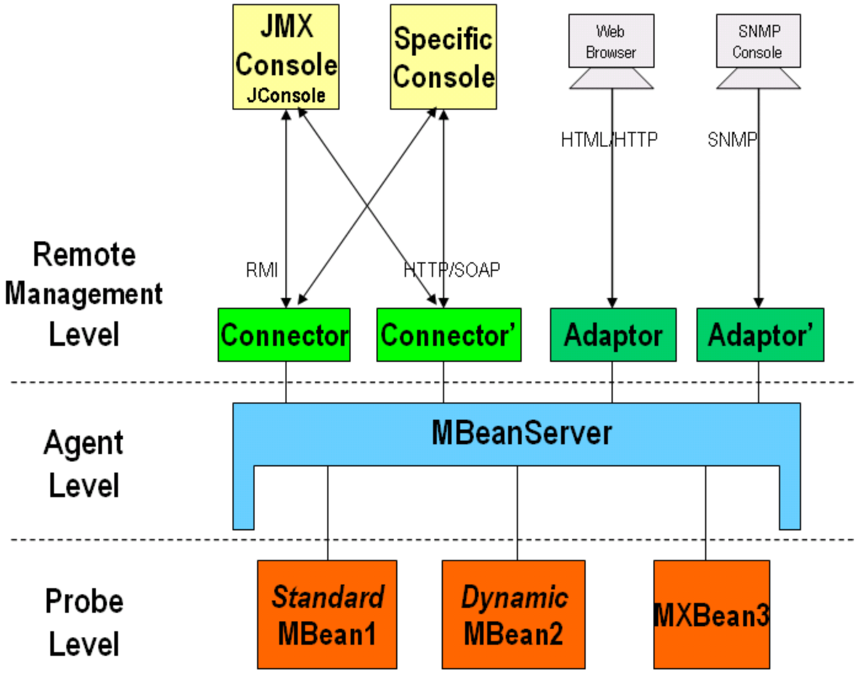
- A collection of open source projects
- Includes the Application Server (AS) and many other components
- Developed by the community
- Released without commercial support
- Very widely deployed

# JBoss Products

- Productized builds based primarily on JBoss project code
- Sold by subscription with commercial support
- Includes backported security patches and coverage from the Red Hat Security Response Team (SRT)
- I work for SRT, responsible for all JBoss products

# JMX (Java Management Extensions)

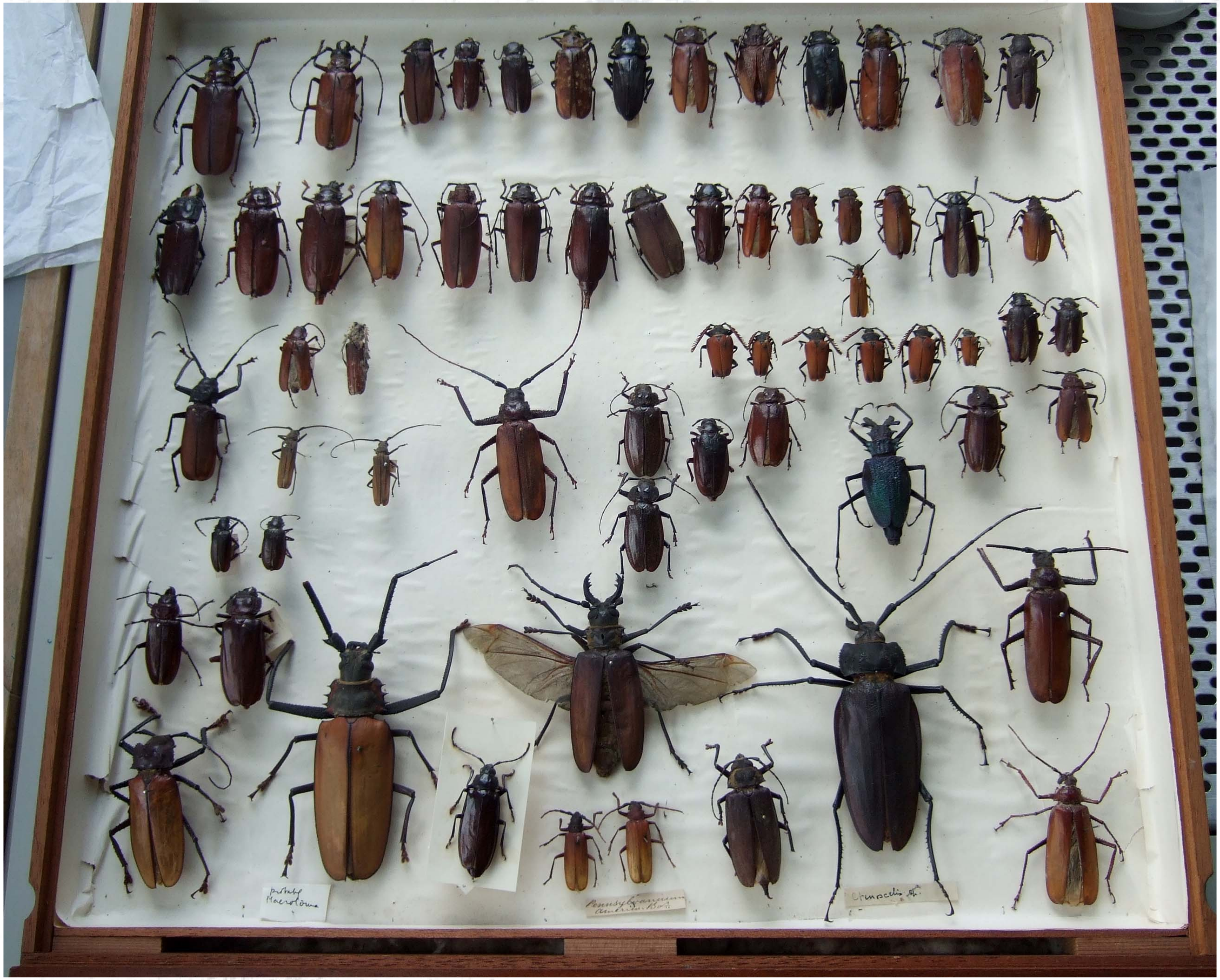
- Framework for managing and monitoring systems via MBeans
- Probe, Agent and Remote Management layers



# JMX Console

- Web-based JMX management interface, shipped with JBoss AS
- Allows a user to invoke methods on MBeans via a web interface
- Included in JBoss AS < 7, EAP and derived products
- Password-based authentication by default on EAP, open by default on AS
- A major attack surface

# Historical Vulnerabilities


probably
Macrotoma
Pennsylvanicum
Amerika Bor.
Ctenoscelis ac.

# CVE-2010-0738

- The JMX console in products includes password authentication by default.
- The relevant <security-constraint> tag included:

```
<http-method>GET</http-method>
<http-method>POST</http-method>
```

- Authentication was not applied to other verbs – e.g. HEAD
- The HEAD handler defaulted to the same code execution path as GET

# CVE-2010-0738

- Unauthenticated requests could be made using the HEAD verb, with the same backend effect as GET
- For JBoss AS, no authentication by default. This means the HEAD requests also work. This is critical as we will see when we come to the worm.

# CVE-2010-4476

- Double.parseDouble in the JRE can get into an infinite loop when converting a number to a double
- For example, use 2.2250738585072012e-308
- Can be used to effect a DoS attack
- Affected Java itself, but also Tomcat/JBoss Web via HTTP headers e.g. q
- Fixed in Tomcat/JBoss Web by no longer using Double.parseDouble for the QoS header
- Separate fix in Java itself

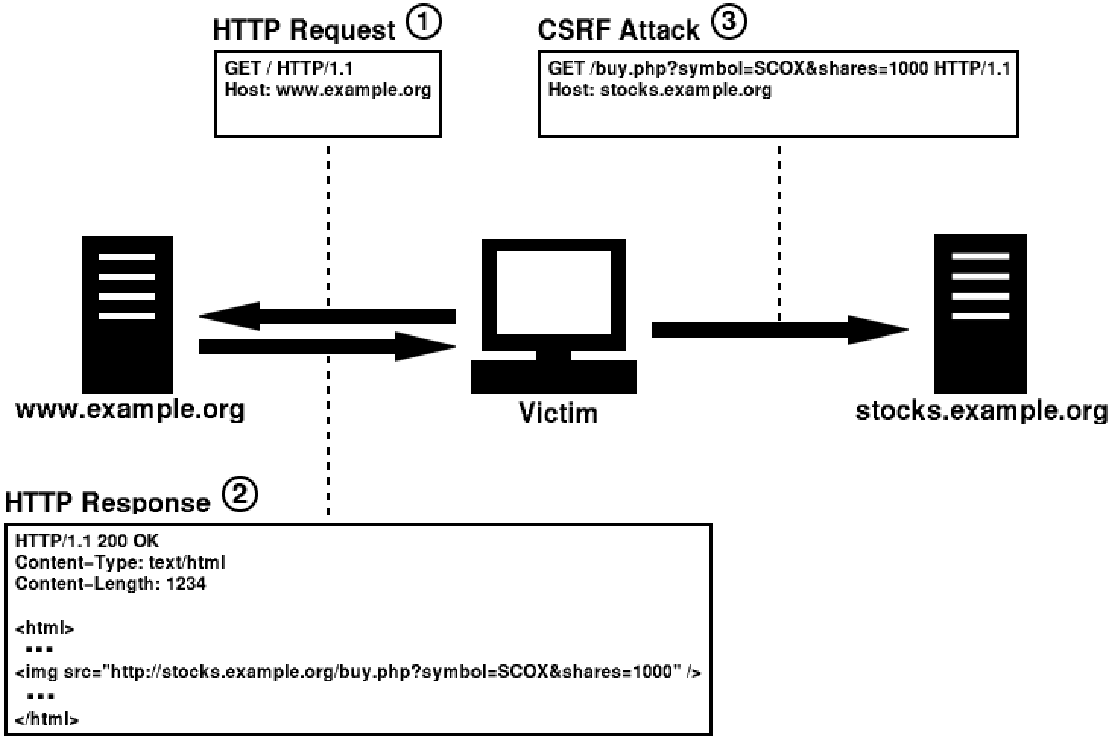
# CVE-2011-1484 / CVE-2011-2196

- Seam did not properly restrict the use of Expression Language (EL) during exception handling.
- An attacker can cause the application to throw an exception, then provide a parameter including EL. The EL can include calls to .class. and .getClass(), which can be used to invoke arbitrary code.
- CVE-2011-1484 was fixed in April 11, but the patch was incomplete and this was found by a user.
- CVE-2011-2196 shipped a complete patch in July 11.
- Both issues handled under embargo – no wild 0day

# CVE-2011-1483

- Remote DoS in jbossws-native (web services)
- An attacker can make a request to XML web services (e.g. SOAP) including recursive entity resolution with embedded DTDs
- The issue was specific to jbossws-native (JBoss), not jbossws-cxf (Apache)
- Enough concurrent attack requests and the server will consume all available connections and die
- Discovered by Red Hat and handled under embargo

# CSRF



```
GET / HTTP/1.1
Host: www.example.org
```

```
GET /buy.php?symbol=SCOX&shares=1000 HTTP/1.1
Host: stocks.example.org
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 1234

<html>
  ...
<img src="http://stocks.example.org/buy.php?symbol=SCOX&shares=1000" />
  ...
</html>
```

Source: talks.php.net

# CVE-2011-2908

- Cross Site Request Forgery (CSRF) against JMX Console
- As shipped with JBoss AS < 7
- Allows a remote attacker to trigger requests by tricking an admin into visiting a malicious URL
- This kind of flaw is often used by real world attackers and pen testers to perform 'spear phishing' attacks.
- Has not been patched at all, even on supported products. A major outstanding flaw.

# CVE-2011-3609

- CSRF against AS7 management console & HTTP API
- By using plain-text JSON calls to the HTTP API, CSRF attacks can be mounted
- Fixed in AS 7.1.0 Beta 1
- Demonstration video...

# Historical Vulnerabilities – Summary

- There are a wide range of flaws covering a wide range of attack surfaces
- The vulnerabilities affect both upstream components and JBoss project code
- The JMX Console and Tomcat/JBoss Web are the source of many issues
- Many lower impact flaws have also been found and fixed: XSS, information disclosure, various DoSes etc.

# Historical Vulnerabilities – Summary

- There are a wide range of flaws covering a wide range of attack surfaces
- The vulnerabilities affect both upstream components and JBoss project code
- The JMX Console and Tomcat/JBoss Web are the source of many issues
- Many lower impact flaws have also been found and fixed: XSS, information disclosure, various DoSes etc.

# JBoss Worm

# JBoss Worm

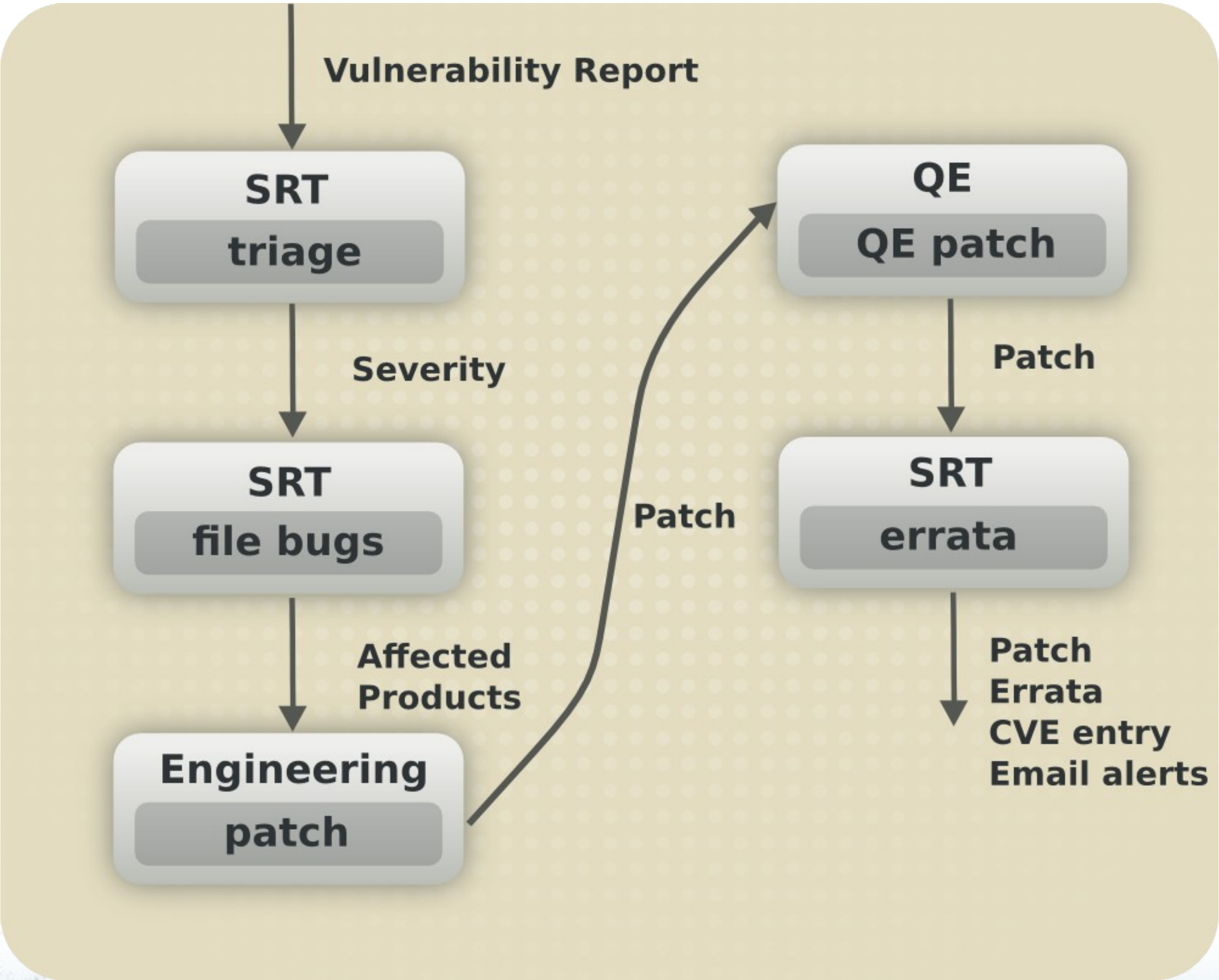
- Exploits CVE-2010-0738, which was patched on supported products in April 2010
- Uses HEAD verb to bypass authentication, then uses the JMX Console to call bshdeployer and deploy arbitrary code to the server
- Installs an IRC-based command and control component for a botnet, then runs a scanner to search random blocks of IP address space for more servers to infect
- Also affects unsecured JBoss AS instances

# JBoss Worm

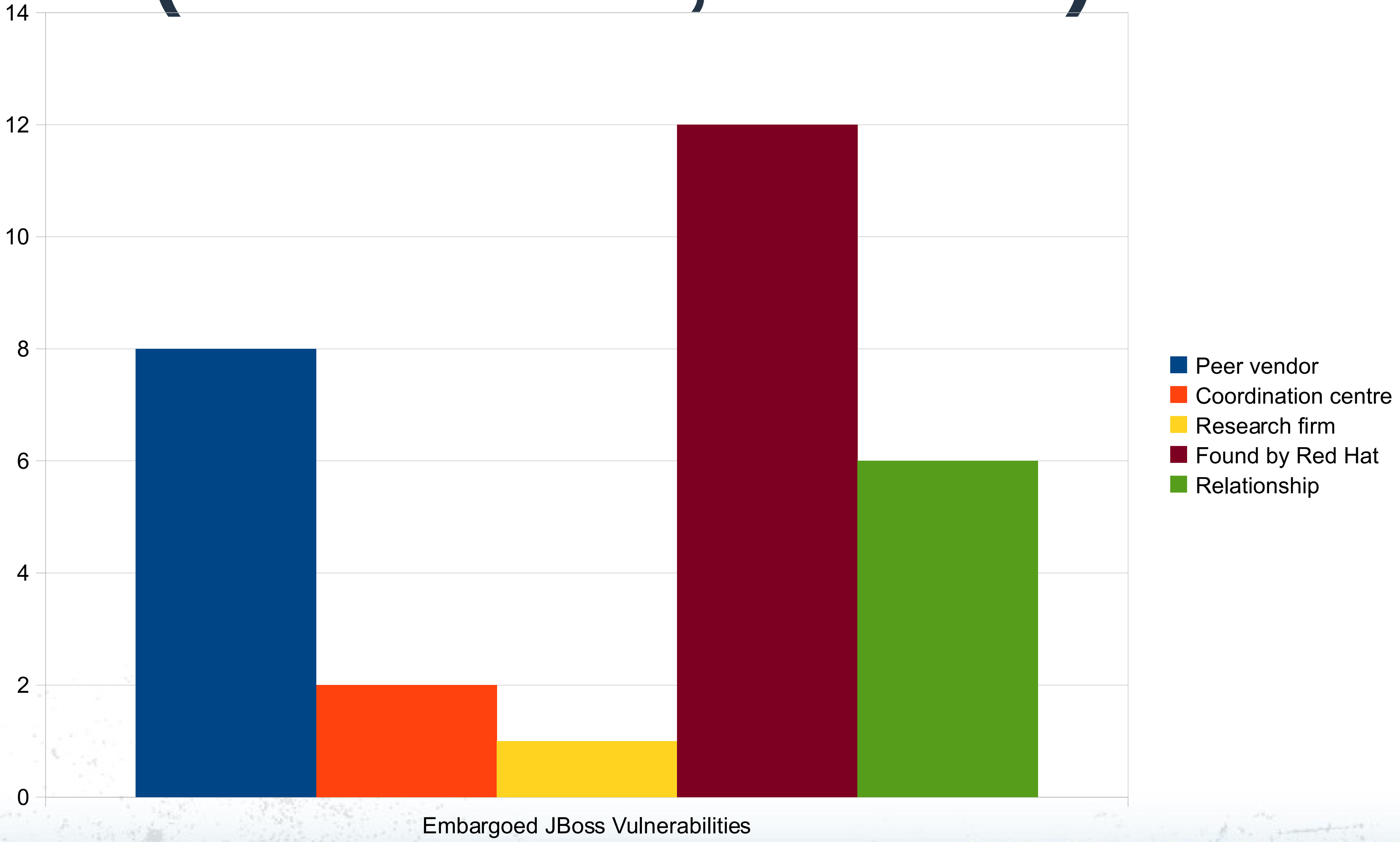
- According to brief google research, most of the affected systems were actually unsecured JBoss AS instances, rather than systems vulnerable to CVE-2010-0738
- This highlights the core problem: if someone is running the latest build of AS7, they will have fixes for all issues that we have patched. If they're running an older version, there's no backporting or async patching.
- People running JBoss AS 5 in production are numerous, and they're getting compromised

# Security Response for Products

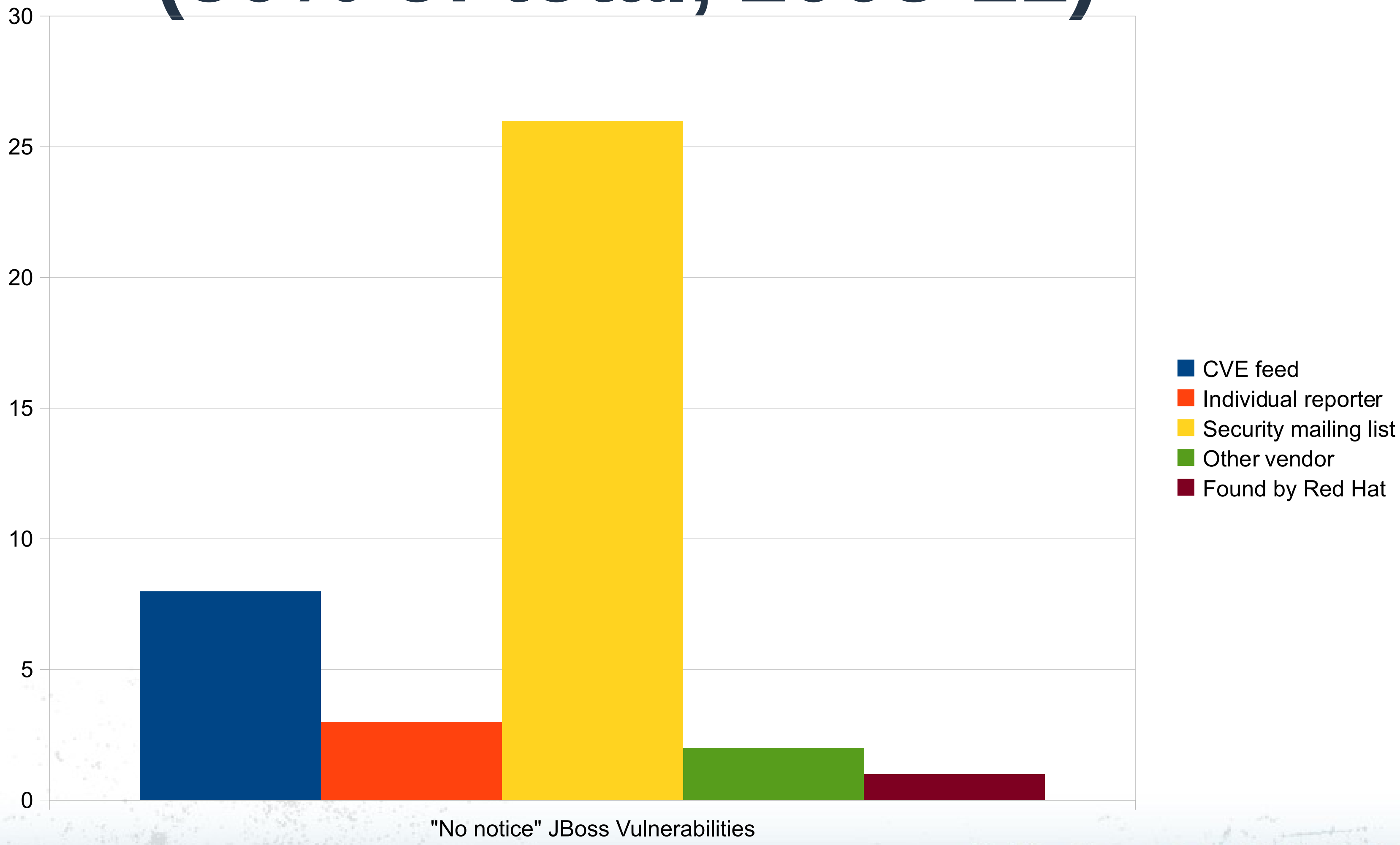
# Security response for products



# Embargoed vulnerabilities (50% of total, 2008-11)



# “No notice” vulnerabilities (50% of total, 2008-11)



# Triage

- Determine whether it affects our products
- Assign a severity (CVSS2)
- Prioritize according to severity
- Assign a CVE ID
- This is the fun part – reproducing bugs, running exploits, feeling the giddy thrill of fresh 0day in your hand

# File Bugs

- Complex bug tracking regime:
- Bugzilla for the whole CVE
- Per-product bugs for affected products. Most in Bugzilla, some in JIRA, one product now heading for EOL was even in Google Code.
- Task bug for monitoring SRT action

# Patch

- Sometimes we produce the patch for our own products
- Especially true for JBoss products with fewer contributors and people sharing the code
- In this case we need to commit our patch back upstream (embargoed)
- Other times we backport it from upstream
- Backporting means cherry picking security fixes

# QE Patch

- Confirm fix solves the security issues
- No regressions introduced
- No performance degradation
- We've had issues with all of the above. A huge cost if we have to clean up one of these impacts after the patch is released.

# Errata

- Packages patch as either an RPM or zip file
- Bundles documentation of the issues
- Available via RHN or CSP
- Triggers alert emails

# The Solution

# The solution

- Secure defaults.

  This is already underway. AS7 has replaced the JMX console and applied security by default. It has also resolved persistent XSS and CSRF issues in the management console:

  `http://community.jboss.org/wiki/AS710Beta1-SecurityEnabledByDefault`

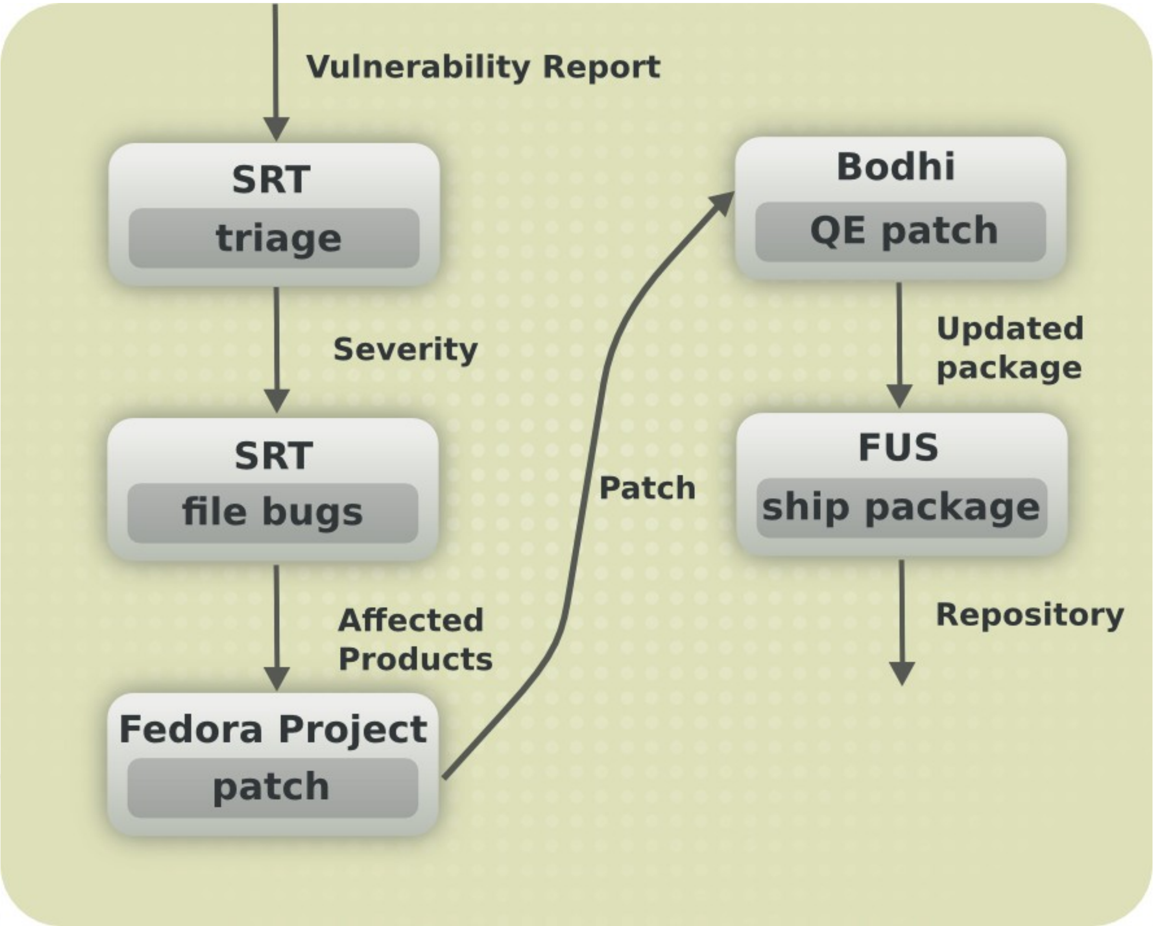
- Security response for projects.

  This would be a whole new undertaking, with various dependencies.

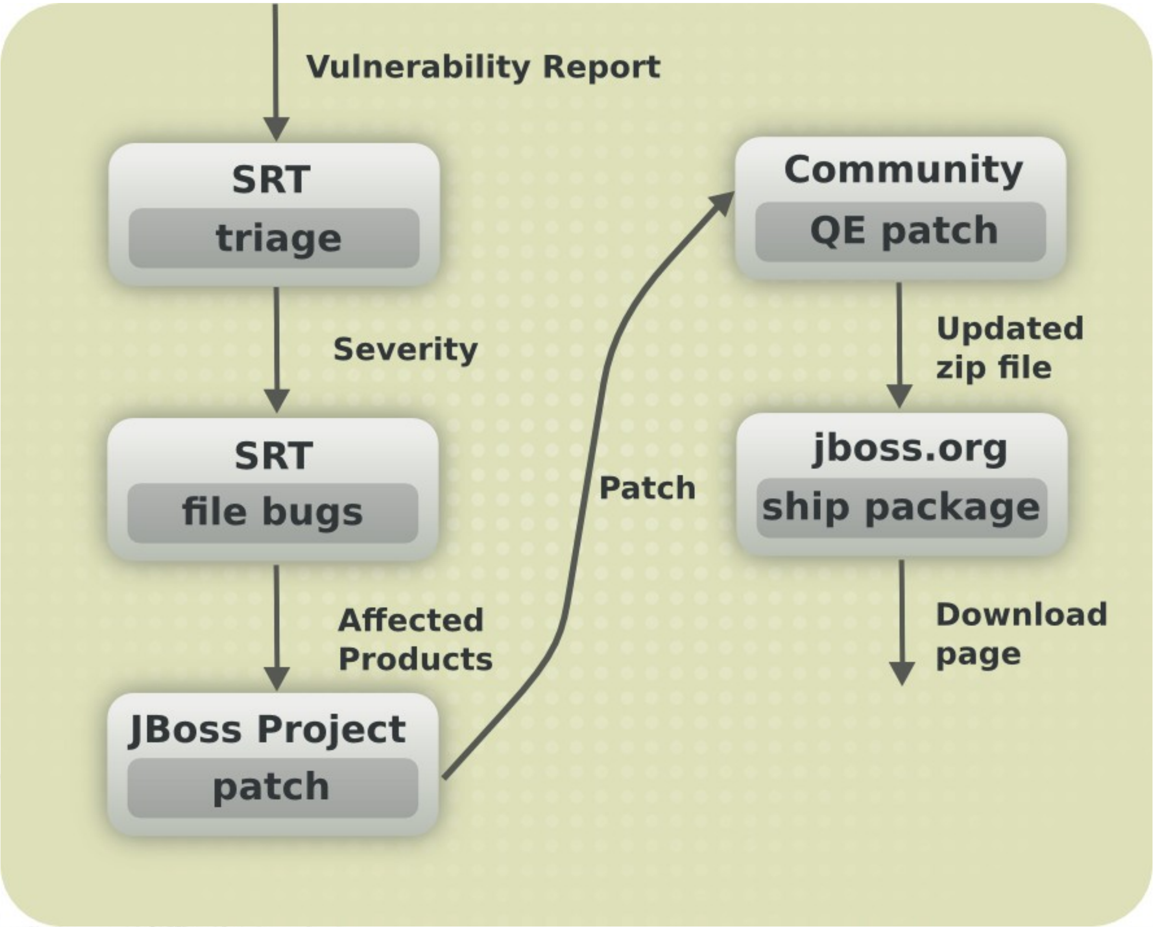
# Security response for projects

- Vision: people no longer need to track the latest release to get all security fixes. Older versions are supported with backported patches through a defined lifecycle
- This is similar to Fedora, so we can learn from that project
- SRT to provide inputs to this process for each flaw
- Optimal solution relies on bugzilla and RPM distribution

# Security response for projects: Fedora model



# Security response for projects: JBoss proposal



# Security response for projects

- Proposed tasks (in sequence)

  1) JBoss AS 7 gets packaged in Fedora

  2) Implement standard Fedora security process, with extra initial SRT assistance

  3) Define lifecycles for JBoss community releases

  4) Implement JBoss project security process, start shipping updated zips with backported patches

  5) Connect downstream projects, e.g. oVirt