

RED HAT :: NASHVILLE :: 2006

SUMMIT



Security Vulnerability Management

Mark J Cox

Responsibility & Accountability

- Unique challenges
 - “The vulnerabilities are there. The fact that somebody in the middle of the night in China who you don't know, quote, "patched" it and you don't know the quality of that, I mean, there's nothing per se that says that there should be integrity that come out of that process.” Steve Ballmer October 2003
- Many vendors all ship the same thing
 - But not exactly the same thing – sometimes not even close
 - and then they backport security fixes too
- Press and researchers often get the facts wrong or deliberately over-sensationalize



Managing vulnerabilities

- Bugs occur across all software applications
 - Some subset have security implications
 - the number and type of vulnerabilities is pretty similar
 - some code is well written and designed for security and some code isn't
- The role of vendors is to add accountability to the process
 - a layer of insulation to provide a stable, secure, platform based on open source technologies
 - Whilst the ability to react is essential, we have



Apache



Apache web server

- Mature project, over 10 years old
- Managed under the legal framework of the Apache Software Foundation
- Powers over half of the Internet web server edge infrastructure
 - (around two-thirds according to Netcraft)
 - (that's over 53 million web sites)
- A critical security flaw would have a significant impact on critical infrastructure
 - at least an impact on consumer confidence





“a loose confederation of programmers ... working in their spare time over gin and tonics at home” -- Wall Street Journal



Apache quality

- Engineers for security
 - You don't find buffer overflow vulnerabilities
- Manages over 1000 contributors
- Standard accountability processes
 - Peer review, Contribution Licenses, release teams, code signing, automated testing and regression tools
- Many vendors ship Apache 'OEM'
 - Apple, HP, IBM, Red Hat, Debian.... increases testing coverage by adding diversity
- Dedicated Security Response Team



Policy



Role of vendors

- An open source architecture is built around a number of applications
 - Red Hat Enterprise Linux provides a complete open source operating environment with web servers, mail servers and client applications such as Open Office
 - (A secure web server is more than just Apache)
- A single point of contact for the security issues affecting every part of that environment
 - Accountability for fixing vulnerabilities that are found with a clear and established response process
 - A single update mechanism for the operating system kernel and applications
 - A single source of advisories



Red Hat Enterprise Linux Errata Life cycle

- 7 years of security errata
 - Asynchronous updates for the highest severity issues
 - Update releases capture lower severity issues
- Each package gets an individual security advisory
 - Asynchronous updates may fix multiple Red Hat Enterprise Linux versions

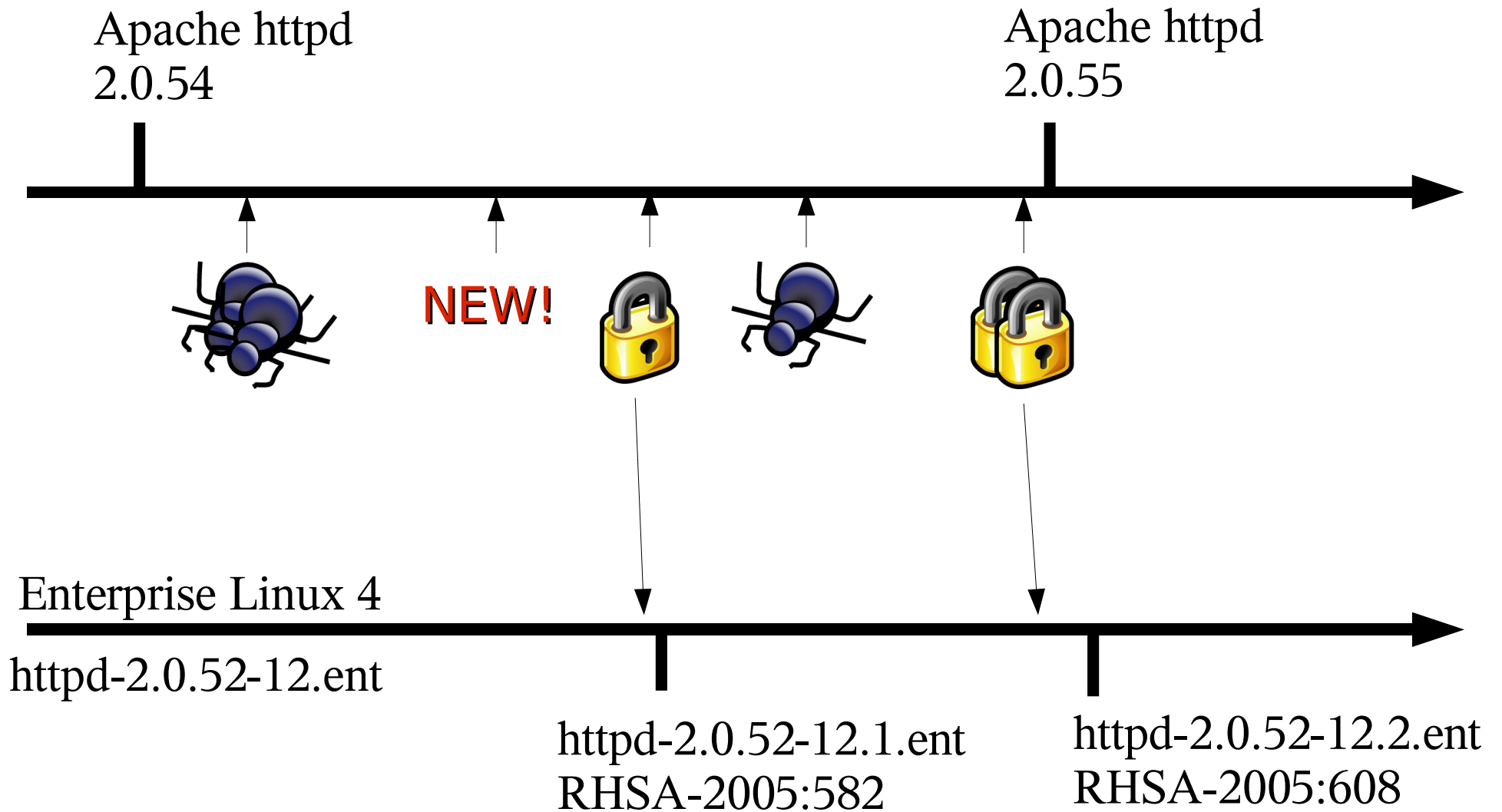
Full Support - 2.5 yrs

Deployment - 3 yrs

Maintenance - 7 yrs

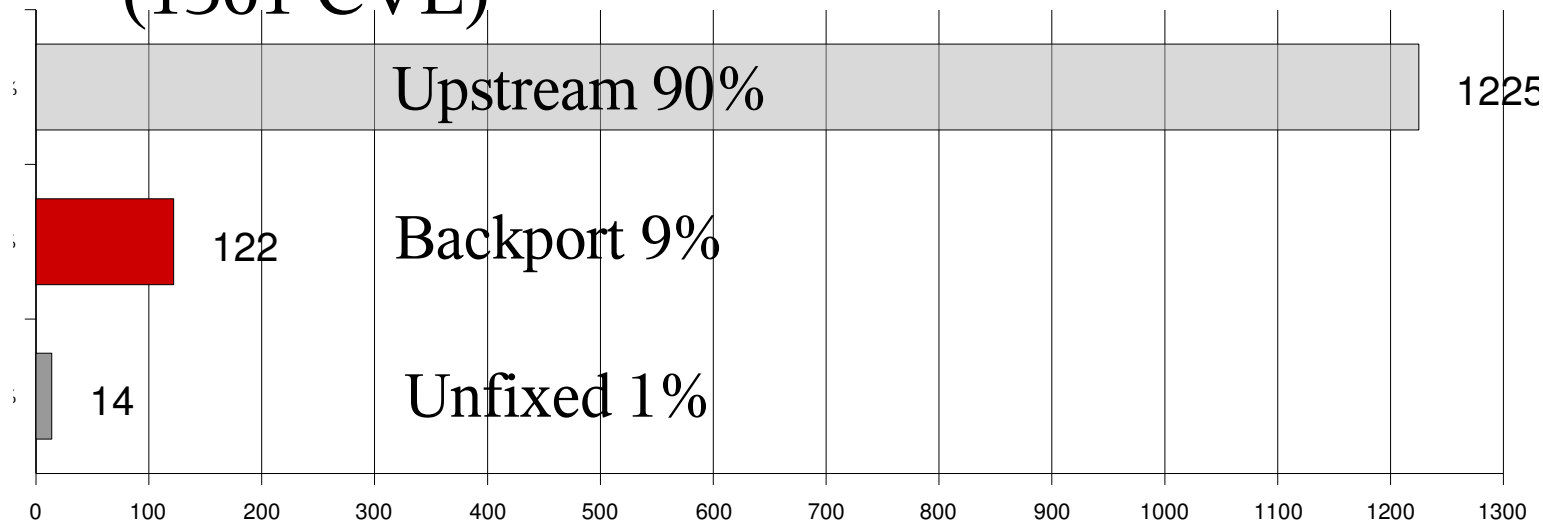


Backporting



Fedora Policy

- A policy of moving upstream, not backporting
 - Might affect the “days of risk” a little
 - Still need some backports for issues not fixed upstream
 - Fedora Core 5 for vulnerabilities Jan 2003 to release (1361 CVE)



Severity Rating

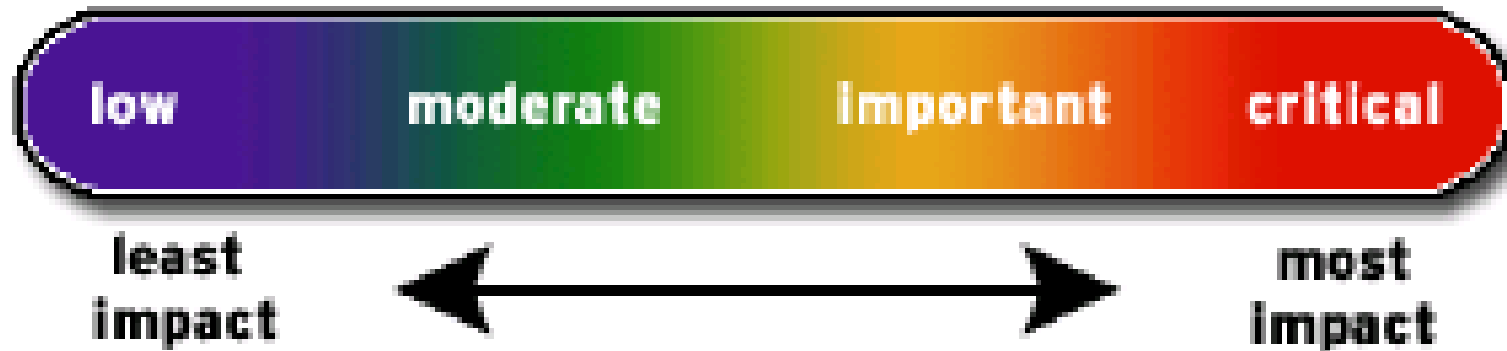


Setting a severity rating

- Based on a technical assessment of the flaw, not the threat
 - Unique to each Red Hat Enterprise Linux distribution
 - Sets the priority through Engineering and QA
 - Trend tracking (source, reported, public)
 - Public in bugzilla “whiteboard” status line
 - Used by internal and external status tools
- Compatible with ranking used by Microsoft and Apache



Severity Rating

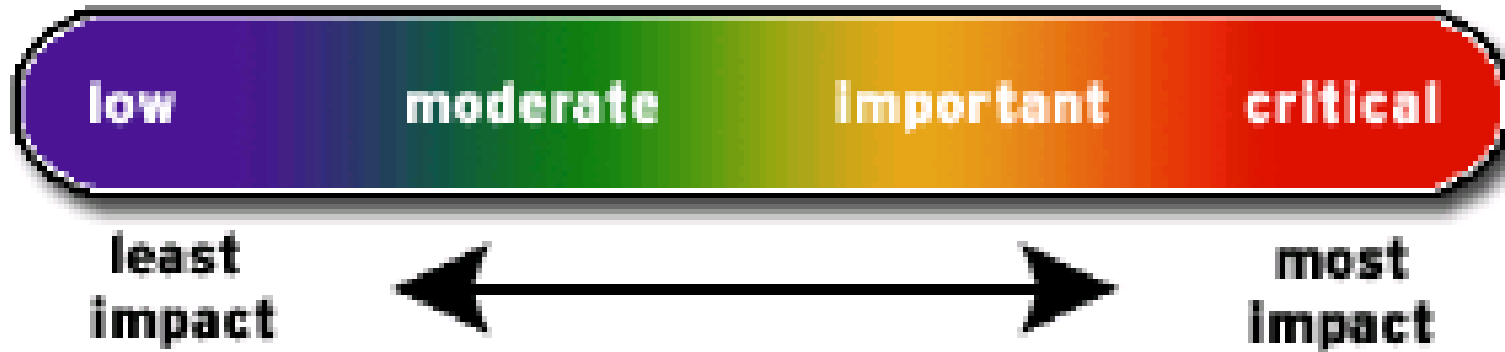


- **Critical**

“A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.”



Severity Rating

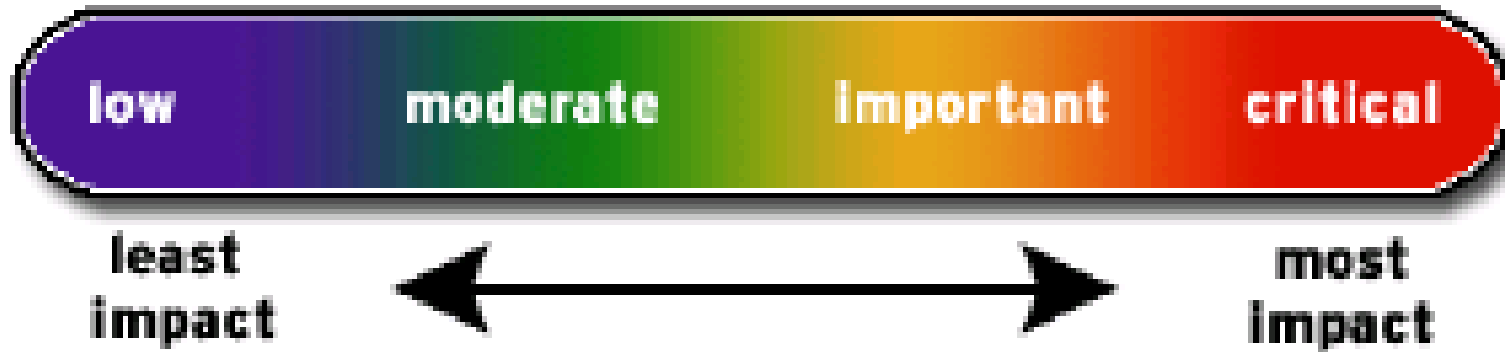


- Important

“easily compromise the Confidentiality, Integrity or Availability of resources”



Severity Rating

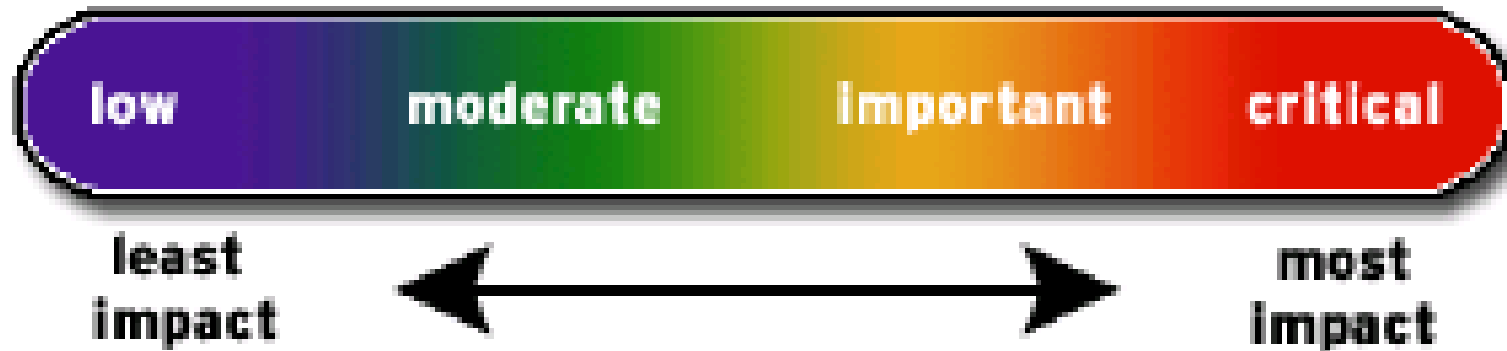


- Moderate

“harder or more unlikely to be exploitable”



Severity Rating



- Low

“unlikely circumstances .. or where a successful exploit would lead to minimal consequences”



Critical Vulnerabilities

- We don't get many
- Those that we get have the potential to create significant risk for customers
- We aim to respond within one working day
- Sometimes this is hard
 - But we are accountable
- Lots of metrics on how many issues and how fast we fixed them in the next session



Where to find our severity ratings

Type	Advisory	Synopsis
	RHSA-2006:0425	Important: libtiff security update
	RHSA-2006:0427	Moderate: ruby security update
	RHSA-2006:0451	Important: xorg-x11 security update
	RHSA-2006:0280	Moderate: dia security update

- For advisories
 - In the advisory, Red Hat Network notifications
- For individual vulnerabilities
 - In bugzilla





Moderate: ruby security update

Bug Comments

Opened by Josh Bressers (Security Response Team)
(bressers@redhat.com)

on 2006-04-20 16:13
EST

Ruby [http/xmlrpc server DoS](#)

Additional Bug Information

A b
ser
ser
oth

Summary

CVE-2006-1931 Ruby http/xmlrpc server DoS

QA Contact

bhuang@redhat.com

URL

Th
[htt](#)

Internal Whiteboard

Status Whiteboard

npact=moderate,reported=20060412,source=redhat,public=20050630

A r
[htt](#)

QA Whiteboard

Devel Whiteboard

Co
will

Keywords

Security

Issue Trackers (Score)

Fixed In

RHSA-2006-0427

Bug 180520 depends on

[Show dependency tree](#)



How to get notifications

- Red Hat Network will notify you of updates needed to packages installed on your systems
 - By email
 - By the up2date applet
 - By logging in
- Subscribing to enterprise-watch-list@redhat.com
- From the web <https://rhn.redhat.com/errata/>
- RSS feed



Security Response Team



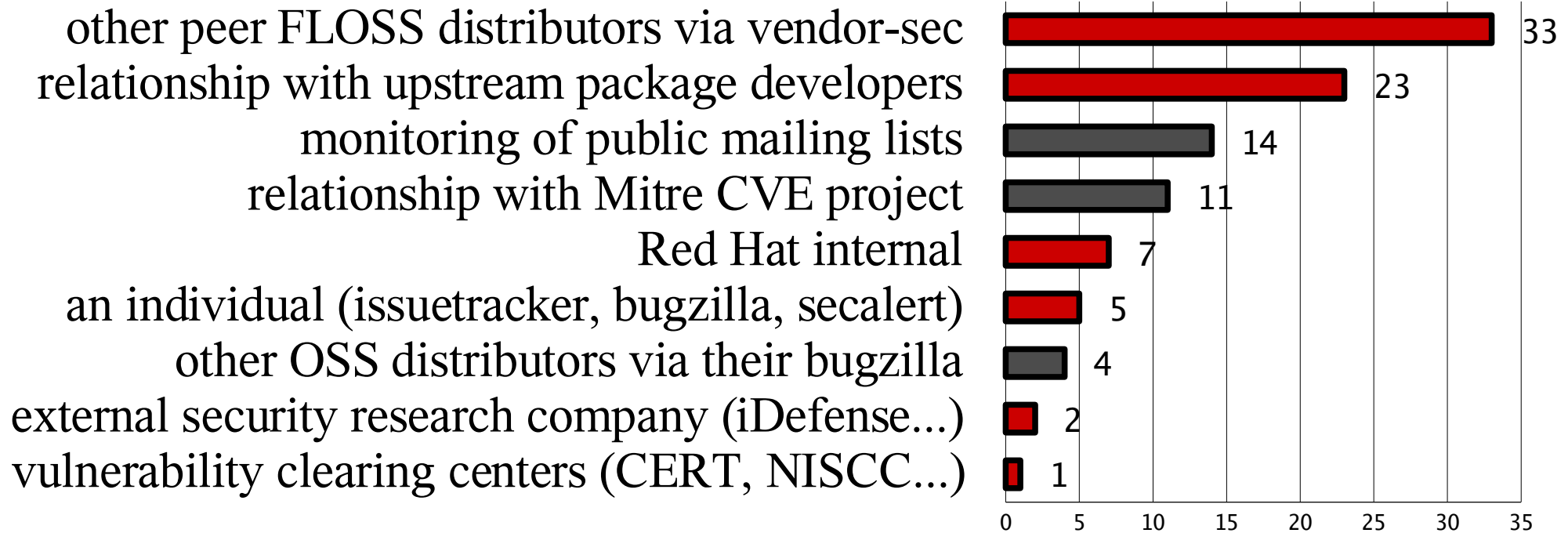
Security Response Team

- Accountable for vulnerabilities that affect Red Hat products and services
 - Monitoring
 - Triage
 - Escalation and troubleshooting through life cycle
 - Communication with other affected vendors
 - Internal communication, documentation, advisory
 - Responsible for errata release
 - Metrics and feedback to Engineering



Monitoring for vulnerabilities

- We find out about security issues in a number of ways (% , March 05-March 06)



secalert@redhat.com

- Address used for internal and external customers to ask security vulnerability related questions
 - Reporting new vulnerabilities
 - Asking how we addressed various vulnerabilities
- Charter to respond within 3 business days
 - For fiscal year 2006 (ending March 2006)
 - 92% responded within one business day
 - 99% by two business days



Triage

- Separate out those issues that matter the most
 - Used to prioritize Engineering, QA, documentation...
- Figure out what we ship that is affected
 - Across all product lines, across all supported products and architectures (and including Fedora).
 - Investigate if any of our security innovations help mitigate
- Issues then have individual bugs generated in bugzilla for tracking
- **~18 incoming vulnerabilities per month**



Release Policy

- For critical vulnerabilities
 - Will be pushed immediately an embargo is lifted, or when passed QE
 - Will be pushed at any time or day
- For important vulnerabilities
 - May be held until reasonable time or day
- For moderate or low vulnerabilities
 - May be held until other issues come up in the same package, or the next Update release



Outreach

- Help Open Source projects deal with vulnerabilities
 - Promote the use of intermediates like NISCC
 - Involvement in industry threat assessment bodies
- Improve quality of projects
 - Working with groups on testing and auditing tools
 - Protocol testing, prioritizing for critical infrastructure
 - Red Hat worked with NISCC and Codenomicon in testing and fixing OpenSSL
- To work with our competitors for common good



Misleading messaging

“Year-to-date for 2005, Microsoft has fixed 15 vulnerabilities affecting Windows Server 2003. In the same time period, for just this year, [Red Hat] Enterprise Linux 3 users have had to patch over 34 vulnerabilities and SuSE Enterprise Linux 9 users have had to patch over 78 vulnerabilities” -- Mike Nash, Microsoft, Feb 2005. <http://www.techweb.com/wire/security/60300209>

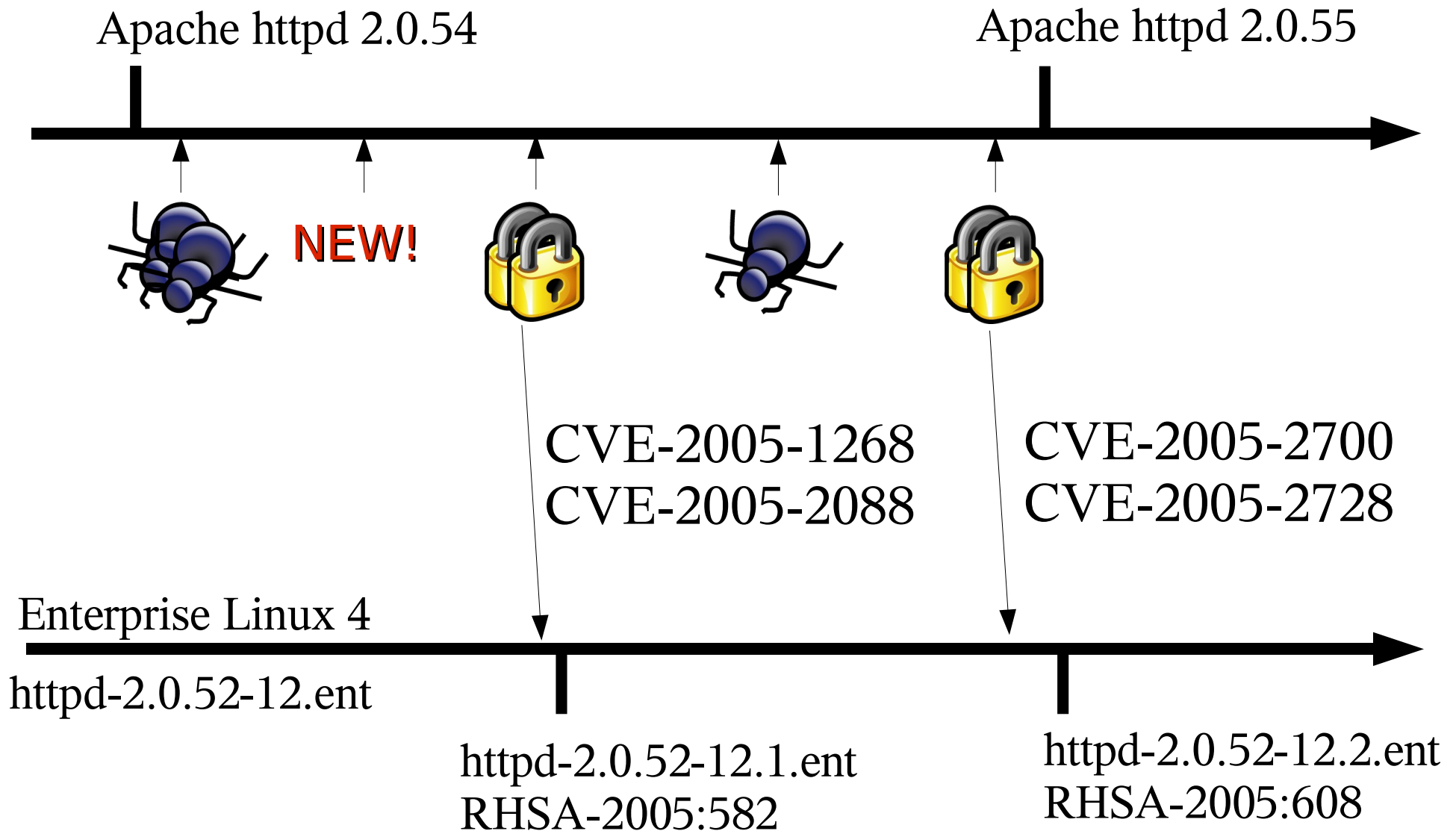
- However, using the Microsoft severity scale:
 - Windows Server 2003 had **three** critical vulnerabilities
 - In Red Hat Enterprise Linux 3 full install had **zero** critical vulnerabilities
- And this only counts their vulnerabilities that actually got disclosed



CVE and OVAL



Review: Backporting



[Apache-SVN] View of /httpd/httpd/branches/2.0.x/CHANGES - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://svn.apache.org/viewcvcs.cgi/httpd/httpd/branches/2.0.x/CHANGES?r


Changes with Apache 2.0.55

*) SECURITY: CVE-2005-2700 (cve.mitre.org)
 mod_ssl: Fix a security issue where "SSLVerifyClient" was not enforced in per-location context if "SSLVerifyClient optional" was configured in the vhost configuration. [Joe Orton]

CVE-2005-2700 (under review) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2700



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Home Get CVE About CVE News and Events Editorial Board Advisory Council Compatible Products

CVE-2005-2700

Additional information is available from the [National Vulnerability Database](#) (also sponsored by [US-CERT](#)).

Name	CVE-2005-2700 (under review)
Status	Candidate
Description	ssl_engine_kernel.c in mod_ssl before 2.8.24, when using "SSLVerifyClient optional" in the global virtual host configuration, does not properly enforce "SSLVerifyClient require" in a per-location context, which allows remote attackers to bypass intended access restrictions.
	<ul style="list-style-type: none"> MLIST:[apache-modssl] 20050902 [ANNOUNCE] mod_ssl 2.8.24-1.3.33 URL:http://marc.theaimsgroup.com/?l=apache-modssl&m=112569517603897&w=2 CONFIRM:http://people.apache.org/~jorton/CAN-2005-2700.diff

Done



rh.n.redhat.com | Red Hat Support - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://rh.n.redhat.com/errata/RHSA

Errata Sign In About RHN

Important: httpd security update

Advisory:	RHSA-2005:608-7
Type:	Security Advisory
Issued on:	2005-09-06
Last updated on:	2005-09-06
Affected Products:	Red Hat Desktop (v. 3) Red Hat Desktop (v. 4) Red Hat Enterprise Linux AS (v. 3) Red Hat Enterprise Linux AS (v. 4) Red Hat Enterprise Linux ES (v. 3) Red Hat Enterprise Linux ES (v. 4) Red Hat Enterprise Linux WS (v. 3) Red Hat Enterprise Linux WS (v. 4)
CVEs (cve.mitre.org):	CVE-2005-2700 CVE-2005-2728

Details

Updated Apache httpd packages that correct two security issues are now available for Red Hat Enterprise Linux 3 and 4.

This update has been rated as having important security impact by the Red

Done

rh.n.redhat.com Adblock

File Edit

Errata

CV

Update

Netwo

Red H

Strong

Strong

Done

lock



Auditing

- Red Hat Network takes care of figuring out what updates you need
- But sometimes you need to use third party tools
 - Local version number comparisons don't work
 - httpd 2.0.55 vs httpd 2.0.52
 - Remote version comparisons are worse
- Screen-scraping our advisories isn't a complete solution





Open Vulnerability and Assessment Language

The language to determine the presence of vulnerabilities and configuration issues on computer systems

- A machine-readable, standard way to express how to detect vulnerabilities and patch issues
 - Definitions contain details of how to test for the presence of vulnerable software
 - can also look for vulnerable uses or configuration
 - XML based standard
 - Modular
 - Designed to deal with heterogeneous environments
 - Interoperability testing of tools and processes



OVAL Compatibility

- From today Red Hat is producing OVAL 5 definitions for all Red Hat Enterprise Linux 3 and 4 security advisories
 - includes definitions for all security advisories to date
 - uses latest (OVAL 5, June 16 2006) schema
 - available on the same day as the advisory (hours)
- Working with MITRE on official compatibility
- <http://oval.mitre.org/>



OVAL example

```
- <advisory from="secalert@redhat.com">
  <severity>Moderate</severity>
  <rights>Copyright 2003 Red Hat, Inc.</rights>
  <issued date="2003-11-12"/>
  <updated date="2003-11-12"/>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0925">CVE-2003-0925</cve>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0926">CVE-2003-0926</cve>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0927">CVE-2003-0927</cve>
</advisory>
</metadata>
- <criteria operator="AND">
  <criteria test_ref="oval:com.redhat.rhsa:tst:20030324001" comment="Red Hat Enterprise Linux 3 is installed"/>
- <criteria operator="OR">
  - <criteria operator="AND">
    <criteria test_ref="oval:com.redhat.rhsa:tst:20030324002" comment="etherreal is earlier than 0:0.9.16-0.30E.1"/>
    <criteria test_ref="oval:com.redhat.rhsa:tst:20030324003" comment="etherreal is signed with Red Hat master key"/>
  </criteria>
- <criteria operator="AND">
  <criteria test_ref="oval:com.redhat.rhsa:tst:20030324004" comment="etherreal-gnome is earlier than 0:0.9.16-0.30E.1"/>
  <criteria test_ref="oval:com.redhat.rhsa:tst:20030324005" comment="etherreal-gnome is signed with Red Hat master key"/>
</criteria>
</criteria>
</criteria>
```

More information

- This is just the reactive side.
- For proactive
 - See the papers from Ulrich Drepper and Dan Walsh from this summit and on the web
- How well did we do?
 - Metrics on our performance, exploits, where the critical flaws were, compromises, and worms in my next presentation in 15 minutes.
- <http://people.redhat.com/mjc/oval/>

