

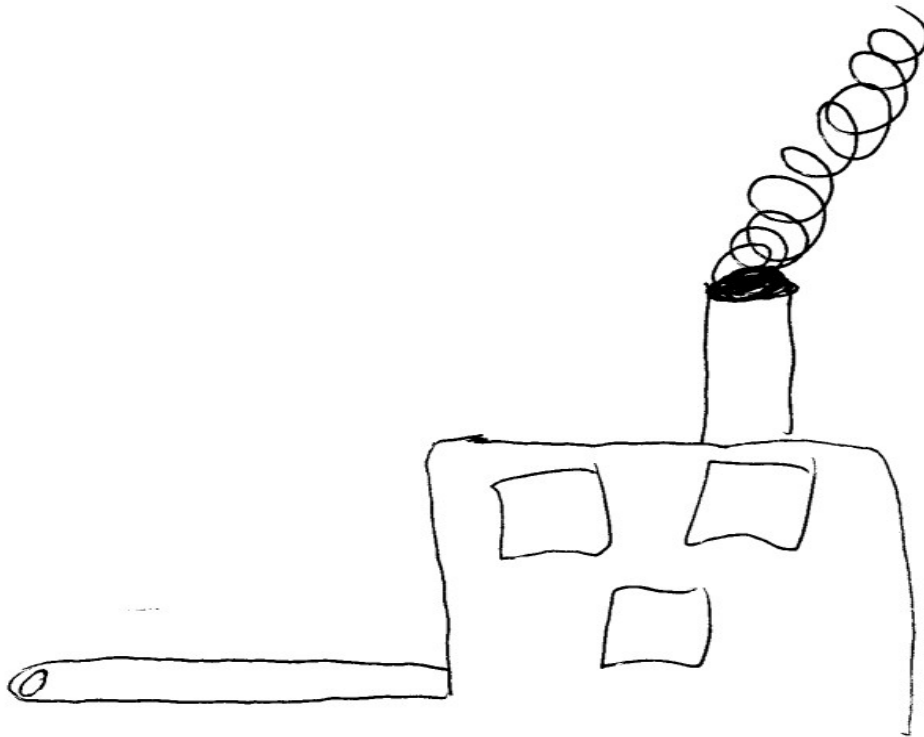


Enterprise Linux Security Errata

Mark Cox, Josh Bressers
Security Response Team, Red Hat

The sausage factory

- the aim of this talk is to explain what goes in, what comes out and some of what happens in the middle





Critical: gnutls security update

Advisory:	RHSA-2008:0489-5
Type:	Security Advisory
Severity:	Critical
Issued on:	2008-05-20
Last updated on:	2008-05-20
Affected Products:	RHEL Desktop Workstation (v. 5 client) Red Hat Enterprise Linux (v. 5 server) Red Hat Enterprise Linux Desktop (v. 5 client)
OVAL:	com.redhat.rhsa-20080489.xml
CVEs (cve.mitre.org):	CVE-2008-1948 CVE-2008-1949 CVE-2008-1950

Details

Updated gnutls packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

This update has been rated as having critical security impact by the Red Hat Security Response Team.

The GnuTLS Library provides support for cryptographic algorithms and protocols such as TLS. GnuTLS includes libtasn1, a library developed for ASN.1 structures management that includes DER encoding and decoding.

Flaws were found in the way GnuTLS handles malicious client connections. A malicious remote client could send a specially crafted request to a service

Managing vulnerabilities

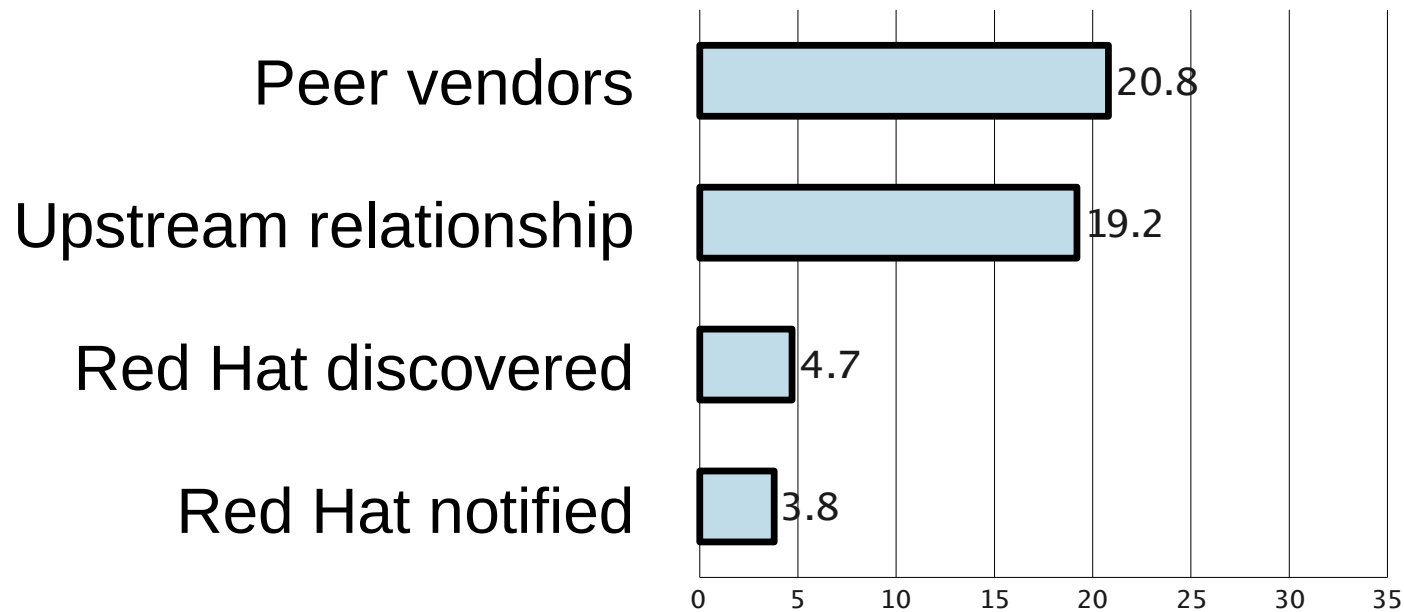
- Bugs occur across all software applications
 - Some subset have security implications
 - some code is well written and designed for security and some code isn't
 - Irrespective of license or source code availability
- The role of vendors is to add accountability to the process
 - a layer of insulation to provide a stable, secure, platform based on open source technologies

“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, 2003

Security Response Team

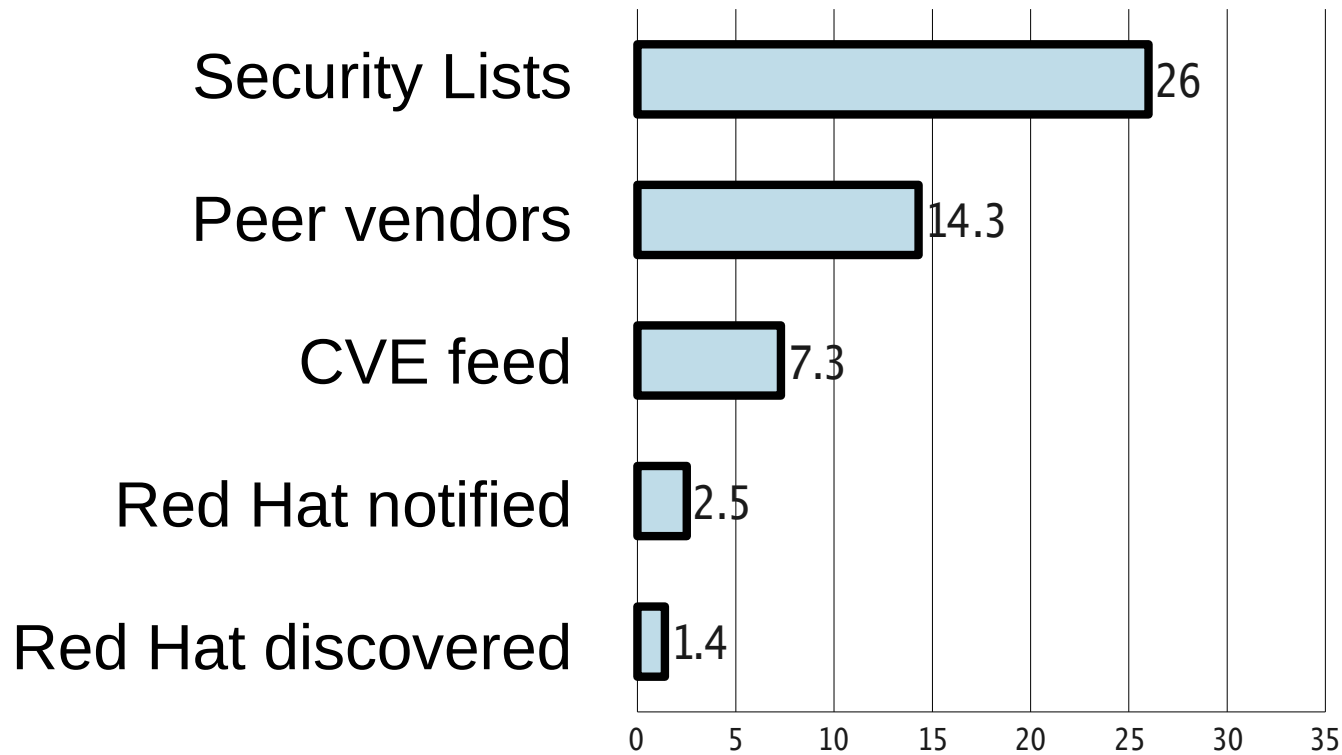
- Accountable for vulnerabilities that affect all Red Hat products and services
 - Monitoring vulnerabilities, exploits, threats
 - Triage
 - Escalation and troubleshooting through life-cycle
 - Communication with other affected vendors
 - Internal communication, documentation, advisory
 - Responsible for errata release
 - Metrics and feedback to Engineering
 - Single point of contact to customers
- Globally distributed diverse team

Monitoring: Embargoed vulnerabilities (48%)



- % total vulnerabilities fixed Enterprise Linux 4, 3 years to March 2008

Monitoring: “no notice” vulnerabilities (52%)



- % total vulnerabilities fixed Enterprise Linux 4, 3 years to March 2008

Triage

- Separate out those issues that matter the most
 - Used to prioritize Engineering, QA, documentation...
- One bug per issue created in bugzilla for tracking
 - “Top level” or “Parent” bug in the “Security Response” product, with alias to the CVE name
- 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

For 2008 we triaged on average
6 vulnerabilities a week

Severity ratings

- Based on a technical assessment of the flaw, not the threat
 - Unique to each vulnerability on each product
 - Sets the priority through Engineering and QA
 - Determines when it will be fixed
- Compatible with ranking used by Microsoft, Apache, others



Critical vulnerabilities

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

- We don't get that many, fortunately
- Those that we get have the potential to create significant risk for customers
- We aim to respond within one working day of the issue being public, even if we didn't get advance notice
- Sometimes this is hard
 - dealt with as emergency



Extending Critical Severity

- We also include issues that require a little user interaction, such as say browsing a malicious web site
 - Matches what other vendors do
 - Although it's not really something a worm can exploit
 - Unless it also affects your HTML email client
 - “don't browse malicious sites” isn't useful advice
- How serious are they really?
 - Lower impact on Unix platforms according to NVD and others
 - Don't run your browser as root



Important vulnerabilities

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

- We aim to have these fixed within a week of them being known to the public
 - but quicker if we had advance notice



Moderate and Low vulnerabilities

“harder or more unlikely to be exploitable”

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

- Moderate
 - Aim to fix within a month, but security team will decide if we're going to do a security update, or wait
 - Likely to be deferred
- Low
 - Even more likely to be deferred or even 'won't fix' for older products



Finding vulnerability severity information

 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2008-1926

Additional Bug Information

Summary CVE-2008-1926 util-linux: audit log injection via login

URL <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1926>

Status Whiteboard source=redhat,reported=20080419,public=20080420,impact=low

Keywords Security

low

moderate

important

critical

least
impact



most
impact

What we fix and what we don't

- Every security issue gets a CVE name
- Not every issue that gets a CVE name is a security issue
 - PHP safe mode
 - “don't do that again” client crashes
 - May be mitigated by some security innovations
- Not all vendors will be affected equally
 - Perhaps they've applied their own patches
 - They might be shipping an older version
 - The platform may have security mitigations

Enterprise Linux Errata Life cycle

- 7 years of security errata
 - Asynchronous updates for the highest severity issues
 - Update releases capture lower severity issues
- “Update” releases during deployment phase
- Comprises several thousand packages
 - Different configurations with different package sets
 - Default and non-default packages

Full Support - 2.5 yrs

Deployment - 3 yrs

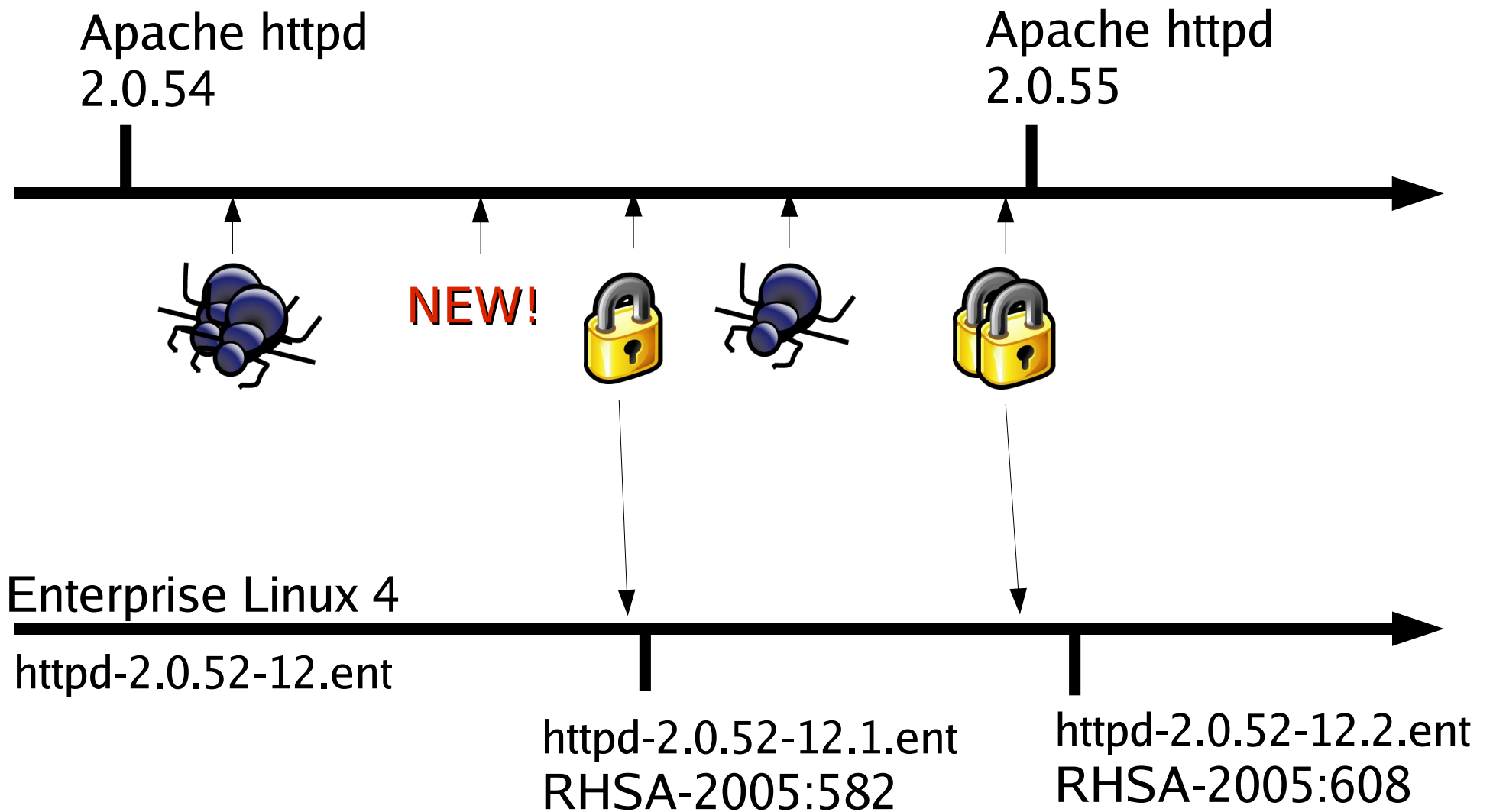
Maintenance - 7 yrs

Deciding to fix

- We've got a set of triaged vulnerabilities, some new, maybe some old deferred low issues
- Fix now?
 - Each package gets an individual security advisory
 - Asynchronous updates may fix multiple Red Hat Enterprise Linux versions
 - But will be split if different severities or different subset of fixes
- Fix later?
 - Defer, pick up in an “Update” release or next async

Backporting

- “Cherry Pick” security fixes from upstream
- Prevents constant upgrading to new versions
 - New version means new bugs
- One small, understood fix
- Speeds turnaround time



Packaging the fix

- Source RPM
 - Contains upstream pristine source
 - Contains patches to that source
 - Available via RHN or FTP
- Shared Libraries
- RPM files are signed with Red Hat key
 - Key shows it has been through standard processes
 - New key since Enterprise Linux 5
 - HSM

```
rpm2cpio httpd-2.2.6-3.src.rpm |  
cpio --make-directories --extract
```

Putting it all together

- Construct the errata
 - Write text
 - Credit Reporters
 - Check information for accuracy
 - Reporters love to embellish
 - “the telephone game”
 - Collate Packages
 - Give to QA
 - Ensure proper testing instructions, reproducers exist
 - This is our “sausage factory”
- Release

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: even holidays/weekends
- For important vulnerabilities
 - May be held until reasonable time or day (Mon-Thu)
- For moderate or low vulnerabilities
 - May be held until other issues come up in the same package, or the next Update release
- No “monthly” schedule
- Same for all 'layered products'

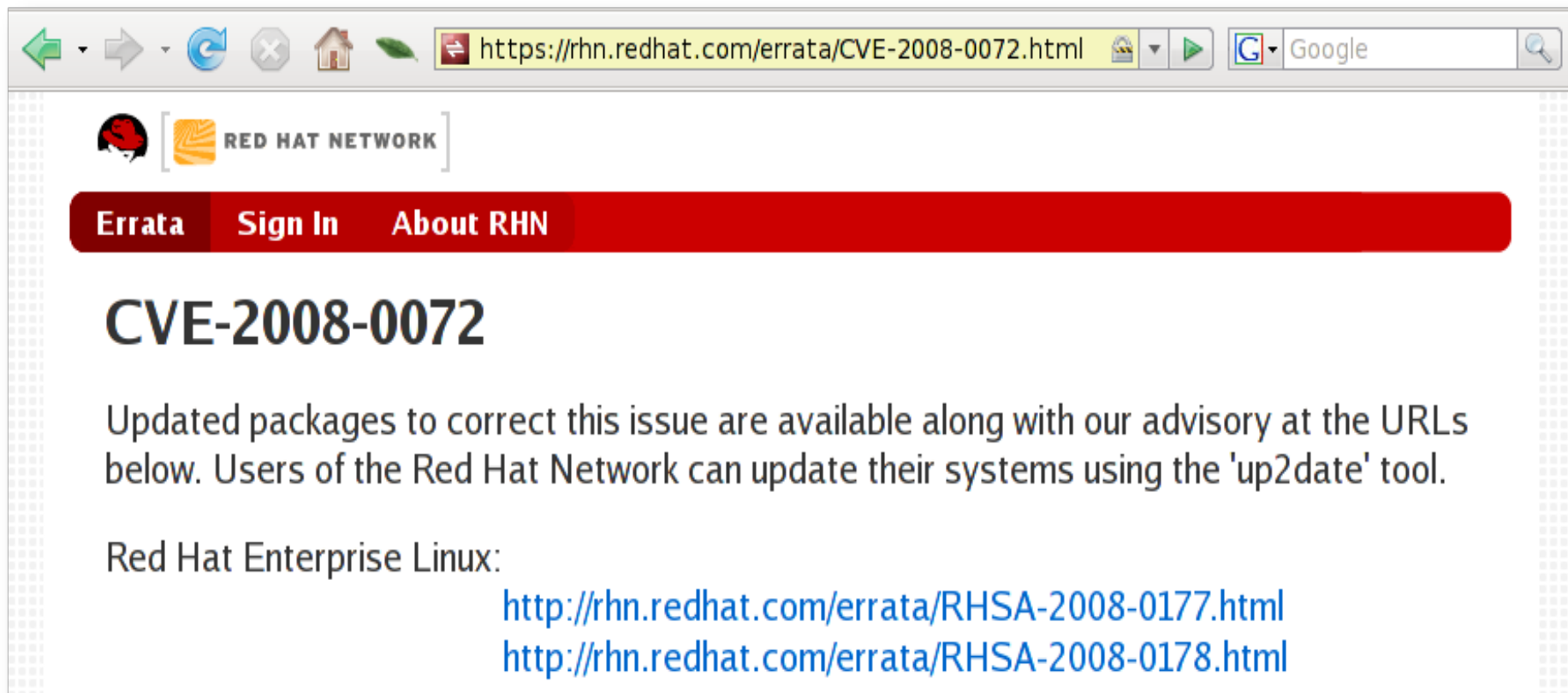
How to get notifications

- Red Hat Network will notify you of updates needed to packages installed on your systems
 - By email if you enable it
 - By up2date/pup
 - By logging in
- Cuts down the number of alerts to those that affect your installation
- Subscribing to enterprise-watch-list@redhat.com or rhsa-announce@redhat.com
 - You can even limit by severity
- From the web <https://rhn.redhat.com/errata/>
- RSS feed



Does an issue affect Red Hat?

- Get the CVE name and use RHN
 - see if we've issued an update already



The screenshot shows a web browser window with the address bar containing the URL <https://rhn.redhat.com/errata/CVE-2008-0072.html>. The browser's search bar contains the word "Google". The page content includes the Red Hat Network logo and navigation links for "Errata", "Sign In", and "About RHN". The main heading is "CVE-2008-0072". The text below the heading states: "Updated packages to correct this issue are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool." Under the heading "Red Hat Enterprise Linux:", there are two blue hyperlinks: <http://rhn.redhat.com/errata/RHSA-2008-0177.html> and <http://rhn.redhat.com/errata/RHSA-2008-0178.html>.

Perhaps it doesn't affect us, try NVD

 <https://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2420>

disclosure of information , Allows disruption of service

Vendor Statements ([disclaimer](#))

Official Statement from Red Hat (5/26/2008)

Not vulnerable. OCSP protocol support was only implemented in upstream stunnel version 4.16. Therefore OCSP protocol is not available in the versions of stunnel as shipped with Red Hat Enterprise Linux 2.1, 3, 4, or 5.

Bugzilla Bug 448290: CVE-2008-2420 stunnel: incorrect CRL verification using OCSP

Alias	CVE-2008-2420	Priority	medium
Product	Security Response Update Products	Severity	medium
Version	unspecified Update Versions	Status	NEW
Component	vulnerability Update Components	Resolution	
OS	Linux	Add CC	
Hardware	All		
Reporter	Tomas Hoger		
Assigned To	Red Hat Security Response Team		

Bug Comments

Opened by Tomas Hoger on 2008-05-25 09:49 EST [\[reply\]](#)

Common Vulnerabilities and Exposures assigned an identifier [CVE-2008-2420](#) to the following vulnerability:

The OCSP functionality in stunnel before 4.24 does not properly search certificate revocation lists (CRL), which allows remote attackers to bypass intended access restrictions by using revoked certificates.

References:

- <http://stunnel.mirt.net/pipermail/stunnel-announce/2008-May/000035.html>
- <http://www.securityfocus.com/bid/29309>
- <http://www.frsirt.com/english/advisories/2008/1569>
- <http://secunia.com/advisories/30335>
- <http://xforce.iss.net/xforce/xfdb/42528>

Comment #1 From Tomas Hoger on 2008-05-25 09:53 EST [\[reply\]](#)

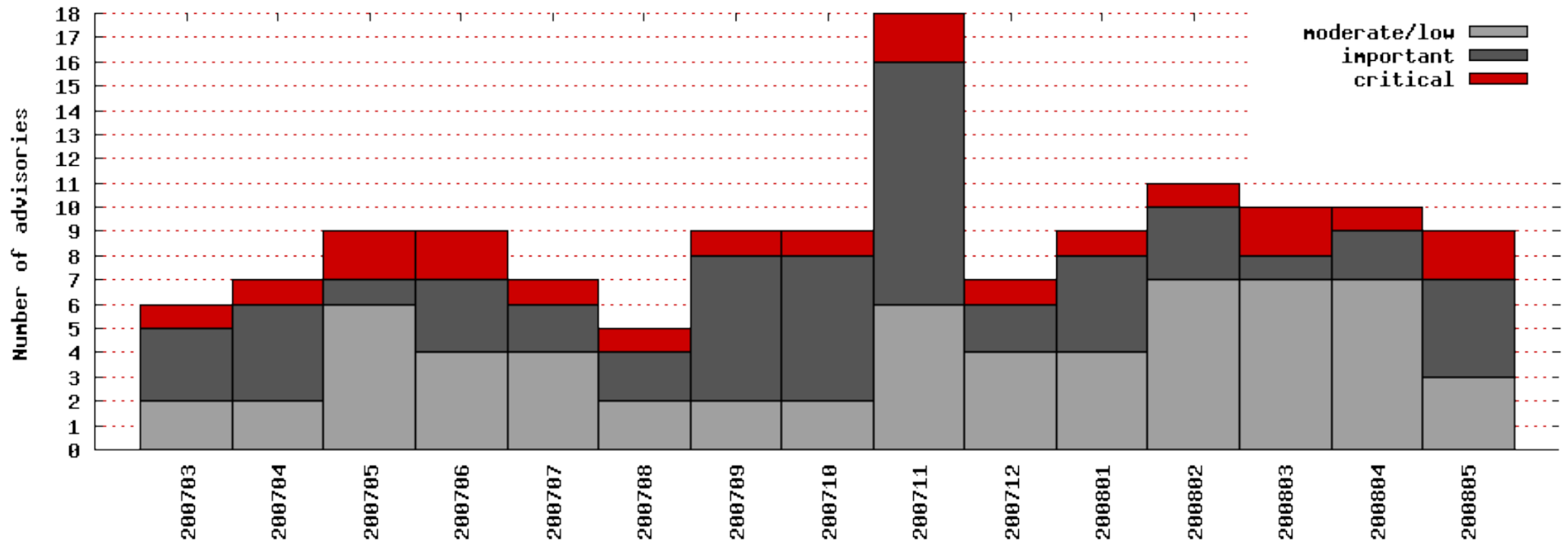
This issue does not affect versions of stunnel as shipped in Red Hat Enterprise Linux 2.1, 3, 4 and 5. Support for OCSP protocol was only implemented in

How to parse an advisory

- Live Examples

How many to parse?

Enterprise Linux 5 Server default install advisories to 20080531



Reducing your exposure

- Remove packages you don't need
 - make a calculated risk 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
 - Why more packages are better (PDF example)
 - PHP Web apps
 - It's why we include Flash and Java in Extras
- SELinux

What to expect in the future

- CVSS v2
 - NVD CVSS ratings and why they're different
 - Use appropriate user accounts
 - Lots of critical issues in user packages such as Firefox
 - So don't run them as root
- CPE
- Integrated “how to find out”
- Mitigation section in advisories

cpe:/o:redhat:enterprise_linux:4:update6

secalert@redhat.com

- Address used to ask security vulnerability related questions
 - Reporting new vulnerabilities
 - Asking how we addressed various vulnerabilities
 - Charter to respond within 3 business days

....or you can ask questions now

Like this session? www.redhat.com/promo/summitfeedback

97%

secalert@redhat.com mails had first response within one business day, Feb 2007- Mar 2008