RED HAT :: CHICAGO :: 2009

SUMMIT

FOLLOW US:

TWITTER.COM/REDHATSUMMIT

TWEET ABOUT US:

ADD #SUMMIT AND/OR #JBOSSWORLD TO THE END OF YOUR EVENT-RELATED TWEET

RED HAT :: CHICAGO :: 2009

SUMMIT

RHSA Secrets Revealed!

Josh Bressers
Senior Software Engineer, Red Hat
2009-09-03

presented by

Today's Topics

What is a security flaw?

What is an RHSA

What gets fixed

How can I find more information about security flaws

The world today

- Security cannot be ignored
- Threats
  - Crackers
  - Worms
  - Botnets
  - Phishers
  - Spammers

Security Bugs

- All software has bugs
  - Some of these bugs have security implications
    - What's the difference?
  - Not all software is written equally
    - Code quality differs between projects

Examples

- Image file that crashes the image viewer
  - Bug (just don't open it again)
- Image file that zips up your home directory and mails it to the bad guys
  - Security flaw
- Crash the computer with a network packet
  - Security flaw
- Crash the computer by smashing it with a hammer
  - Not a security flaw (probably not a bug either)

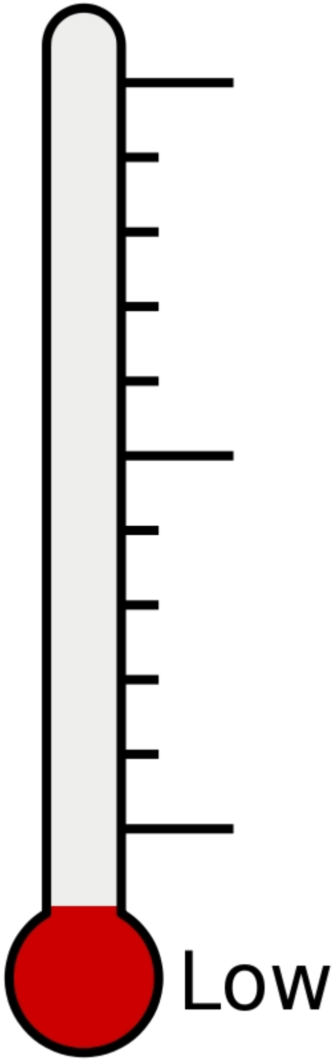
Organizing our bugs

- Every security issue gets a CVE id
- Not all CVE ids are security issues
  - Vendor disputes
  - MITRE is often quite liberal with CVE assignment
- Not every CVE id affects us

Deciding what to fix

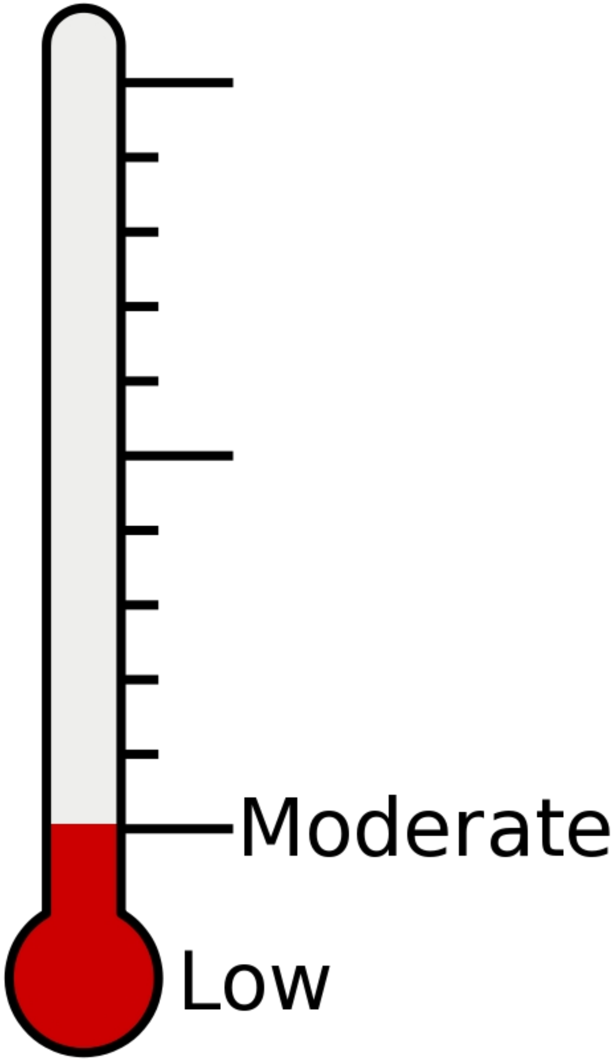
- We have a set of issues
  - Some new, some old
- Fix it now?
- Fix it later?
- We have finite resources, flaws must be prioritized and dealt with in a sensible order

Bug Severities



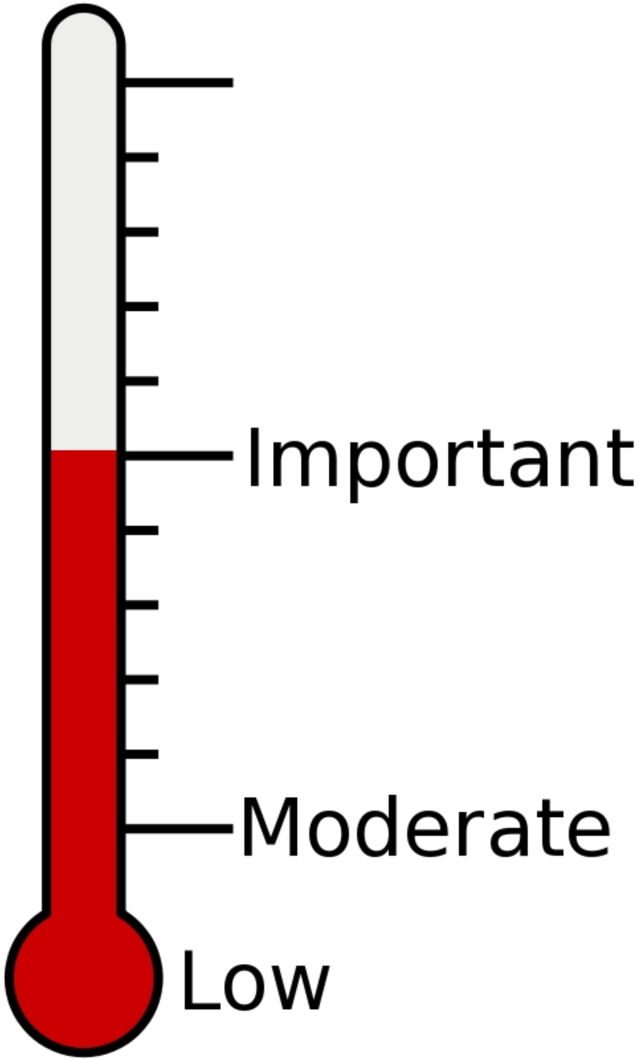
“unlikely circumstances .. or where a successful exploit would lead to minimal consequences”

Bug Severities



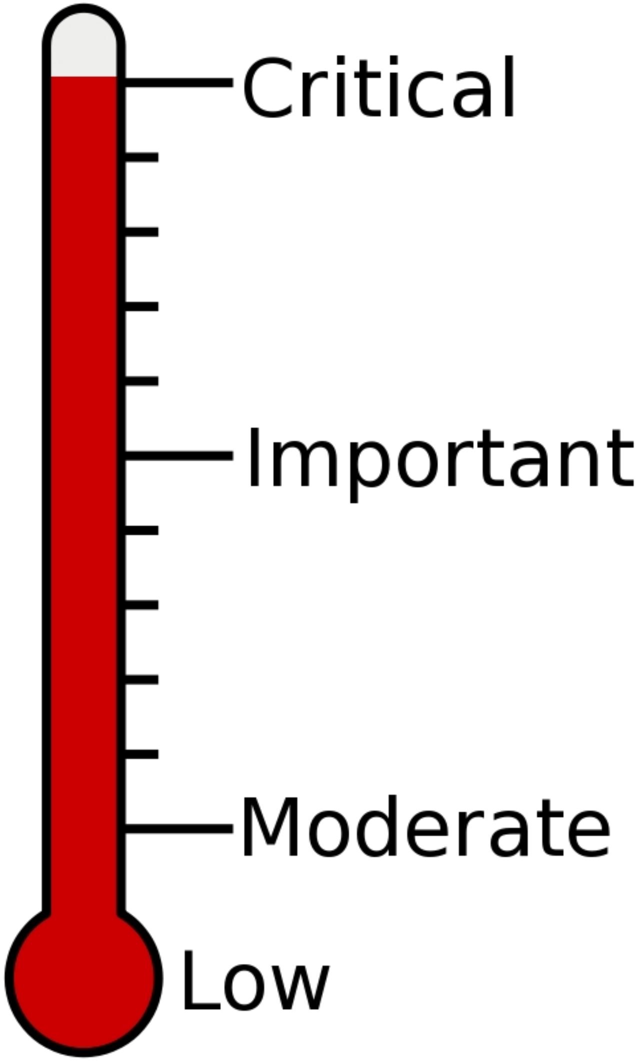
“harder or more unlikely to be exploitable”

Bug Severities



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

Bug Severities

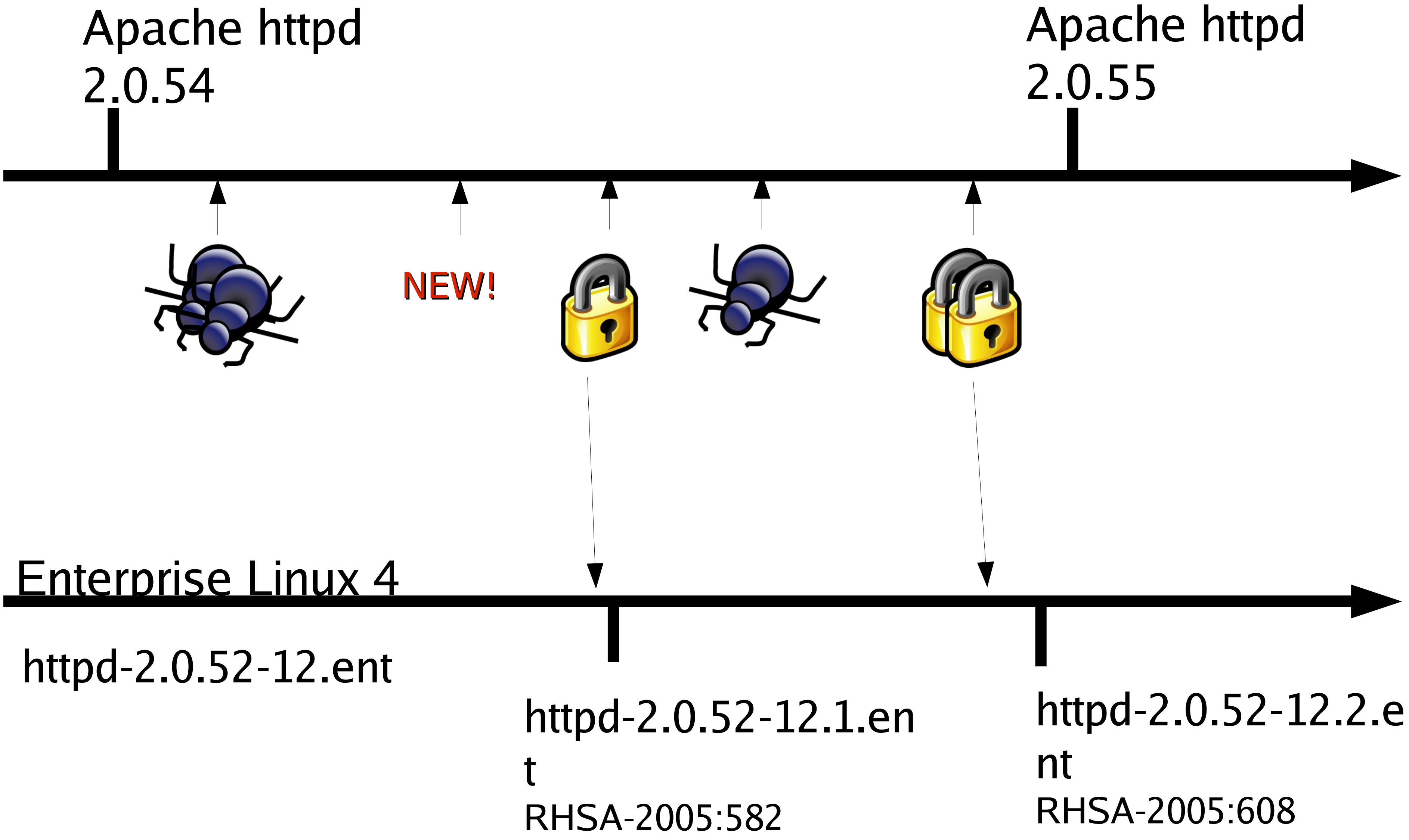


“A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.”

How do we fix it?

- Backport the patch
- Upgrade
  - This is not common
- The update is bundled in a security advisory

How Does Backporting Work?



Apache httpd 2.0.54

Apache httpd 2.0.55

NEW!

Enterprise Linux 4

httpd-2.0.52-12.ent

httpd-2.0.52-12.1.ent
RHSA-2005:582

httpd-2.0.52-12.2.ent
RHSA-2005:608

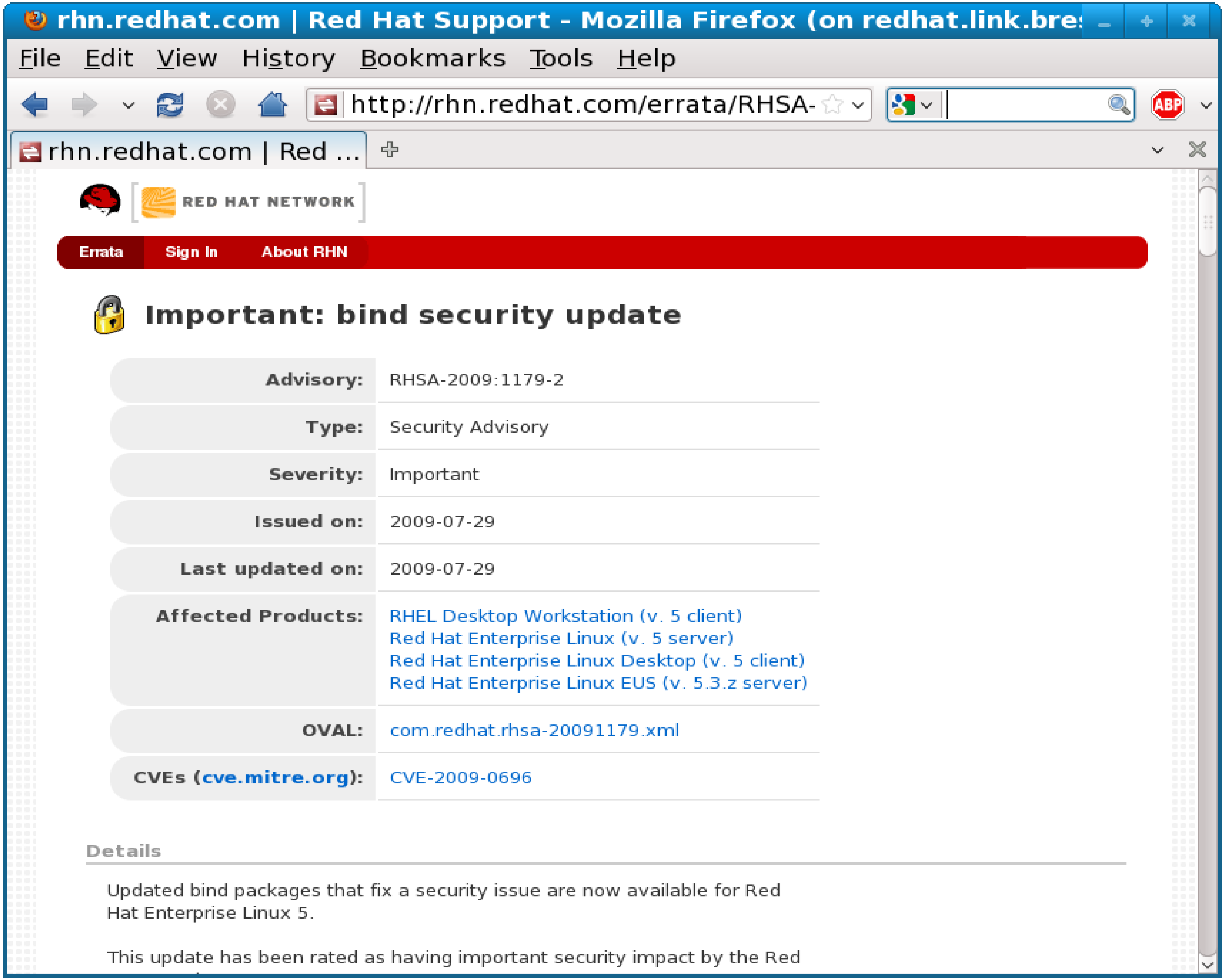
What is an RHSA?

- **R**ed **H**at **S**ecurity **A**dvisory
- Special Errata that fix security flaws
  - Sometimes bugs too
- Released when an update is ready
  - No pre-defined update schedule

What's in an RHSA?

- Header
- Details
- Solution
- Updated Packages
- Bugs Fixed
- References

Errata Header


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bre:
File Edit View History Bookmarks Tools Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...
RED HAT NETWORK
Errata
Sign In
About RHN

Important: bind security update

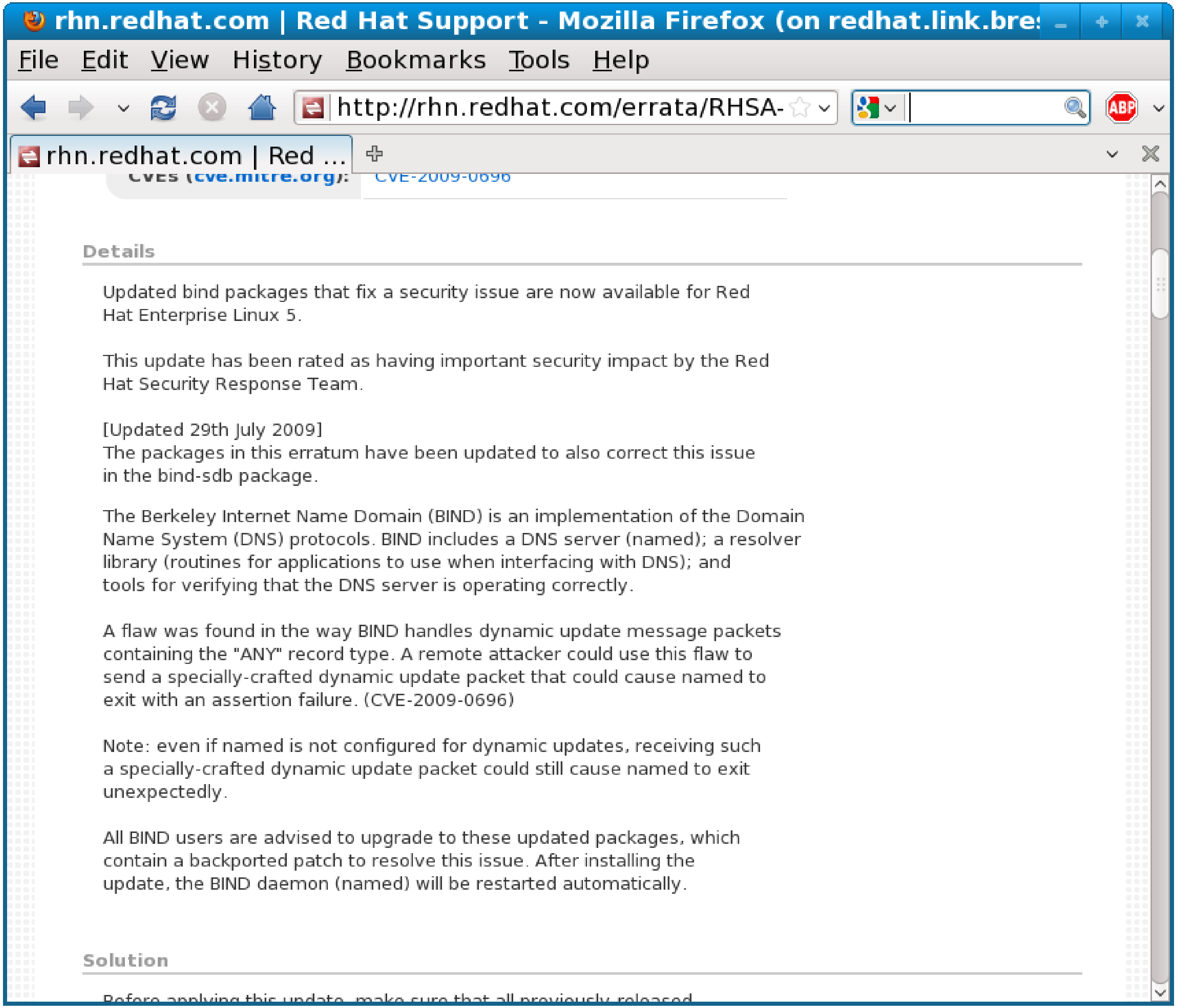
Advisory:	RHSA-2009:1179-2
Type:	Security Advisory
Severity:	Important
Issued on:	2009-07-29
Last updated on:	2009-07-29
Affected Products:	RHEL Desktop Workstation (v. 5 client) Red Hat Enterprise Linux (v. 5 server) Red Hat Enterprise Linux Desktop (v. 5 client) Red Hat Enterprise Linux EUS (v. 5.3.z server)
OVAL:	com.redhat.rhsa-20091179.xml
CVEs (cve.mitre.org):	CVE-2009-0696

Details

Updated bind packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

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

Details


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bre
File Edit View History Bookmarks Tools Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...

CVEs (cve.mitre.org): CVE-2009-0696

Details

Updated bind packages that fix a security issue are now available for Red Hat Enterprise Linux 5.

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

[Updated 29th July 2009]
The packages in this erratum have been updated to also correct this issue in the bind-sdb package.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

A flaw was found in the way BIND handles dynamic update message packets containing the "ANY" record type. A remote attacker could use this flaw to send a specially-crafted dynamic update packet that could cause named to exit with an assertion failure. (CVE-2009-0696)

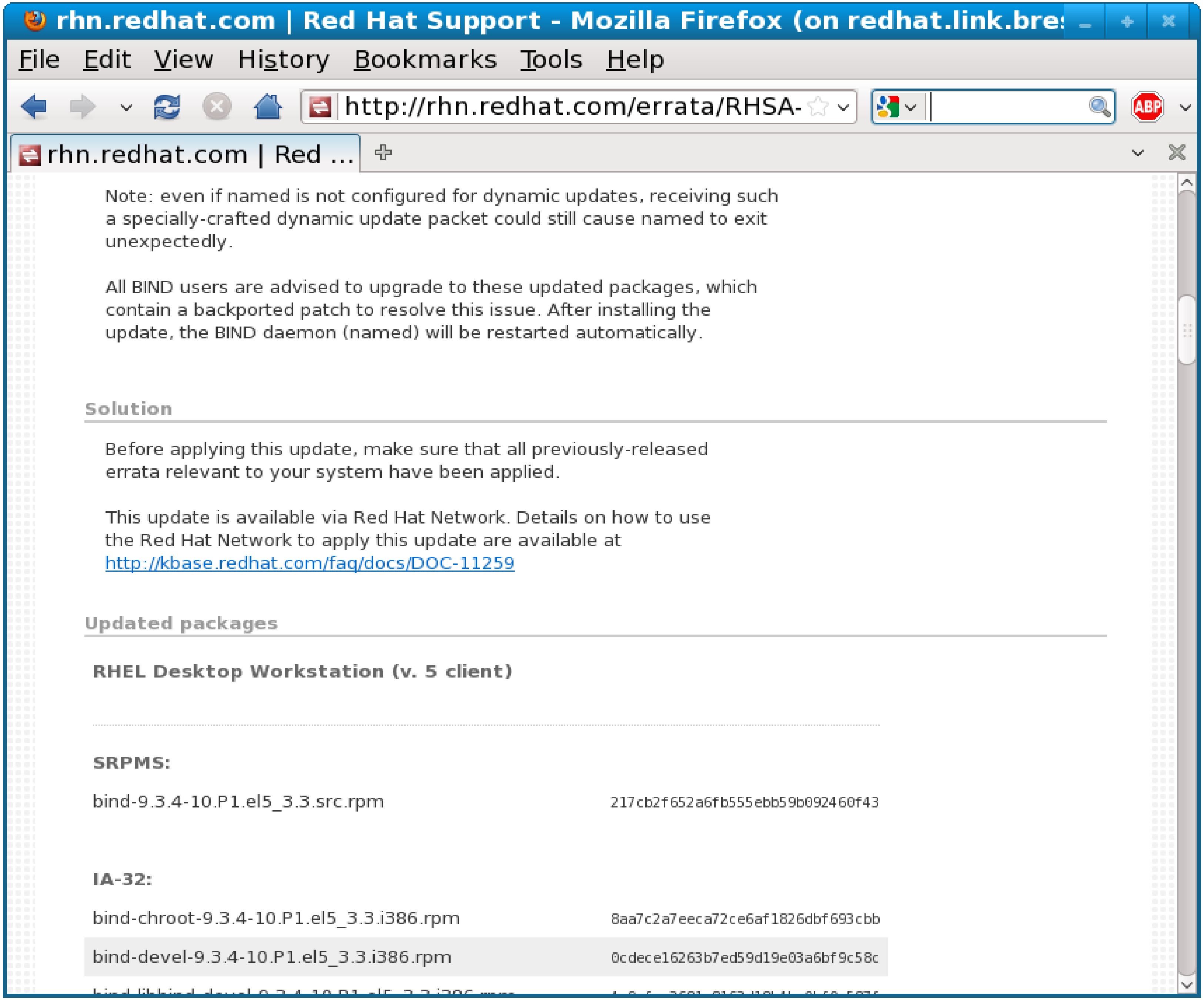
Note: even if named is not configured for dynamic updates, receiving such a specially-crafted dynamic update packet could still cause named to exit unexpectedly.

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

Solution

Before applying this update, make sure that all previously released

Solution


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bres
File Edit View History Bookmarks Tools Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...
ABP

Note: even if named is not configured for dynamic updates, receiving such a specially-crafted dynamic update packet could still cause named to exit unexpectedly.

All BIND users are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

Solution

Before applying this update, make sure that all previously-released errata relevant to your system have been applied.

This update is available via Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at http://kbase.redhat.com/faq/docs/DOC-11259

Updated packages

RHEL Desktop Workstation (v. 5 client)

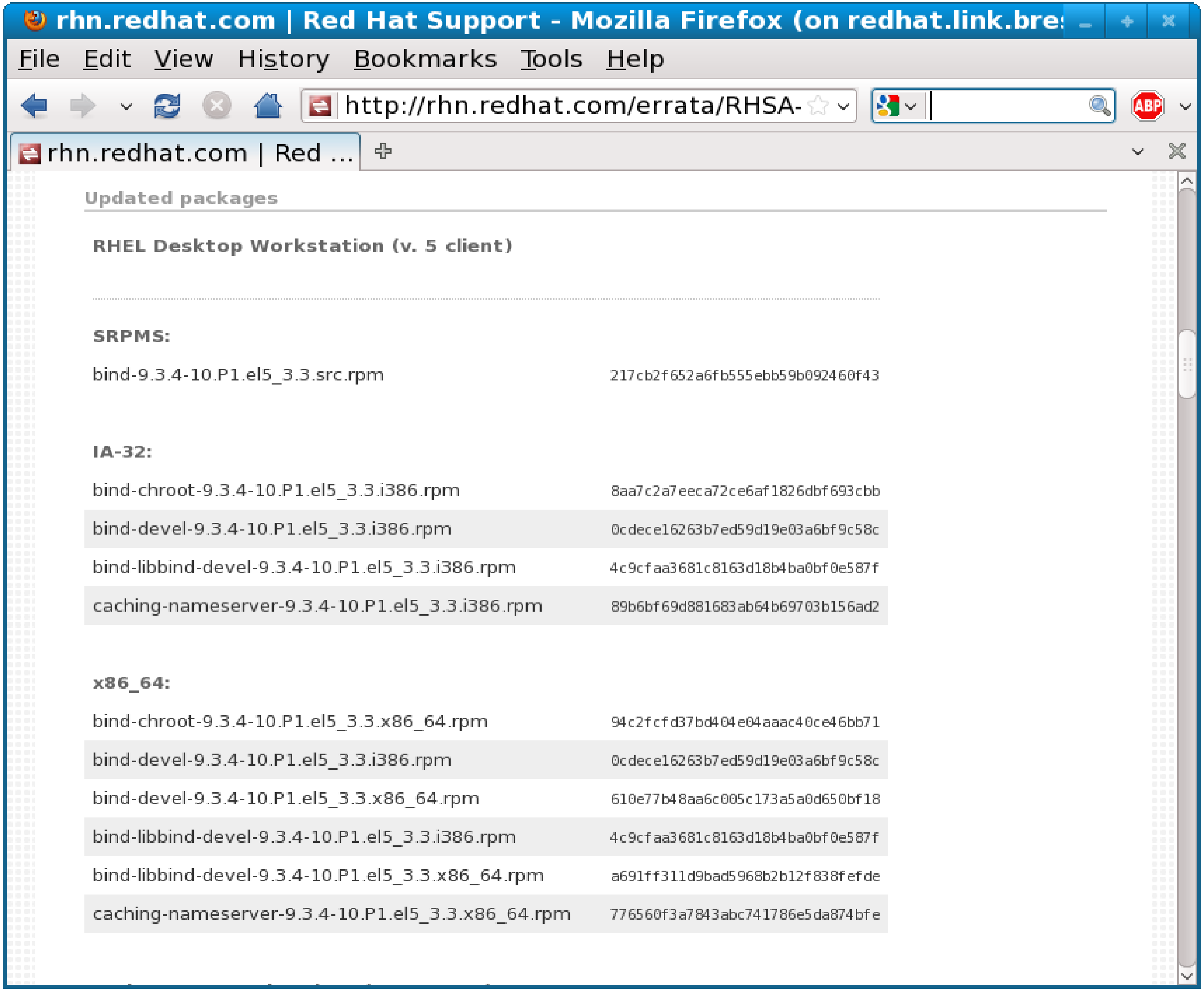
SRPMS:

bind-9.3.4-10.P1.el5_3.3.src.rpm	217cb2f652a6fb555ebb59b092460f43

IA-32:

bind-chroot-9.3.4-10.P1.el5_3.3.i386.rpm	8aa7c2a7eeca72ce6af1826dbf693cbb
bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm	0cdece16263b7ed59d19e03a6bf9c58c

Updated Packages


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bre:
File Edit View History Bookmarks Tools Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...

Updated packages

RHEL Desktop Workstation (v. 5 client)

SRPMS:

bind-9.3.4-10.P1.el5_3.3.src.rpm	217cb2f652a6fb555ebb59b092460f43

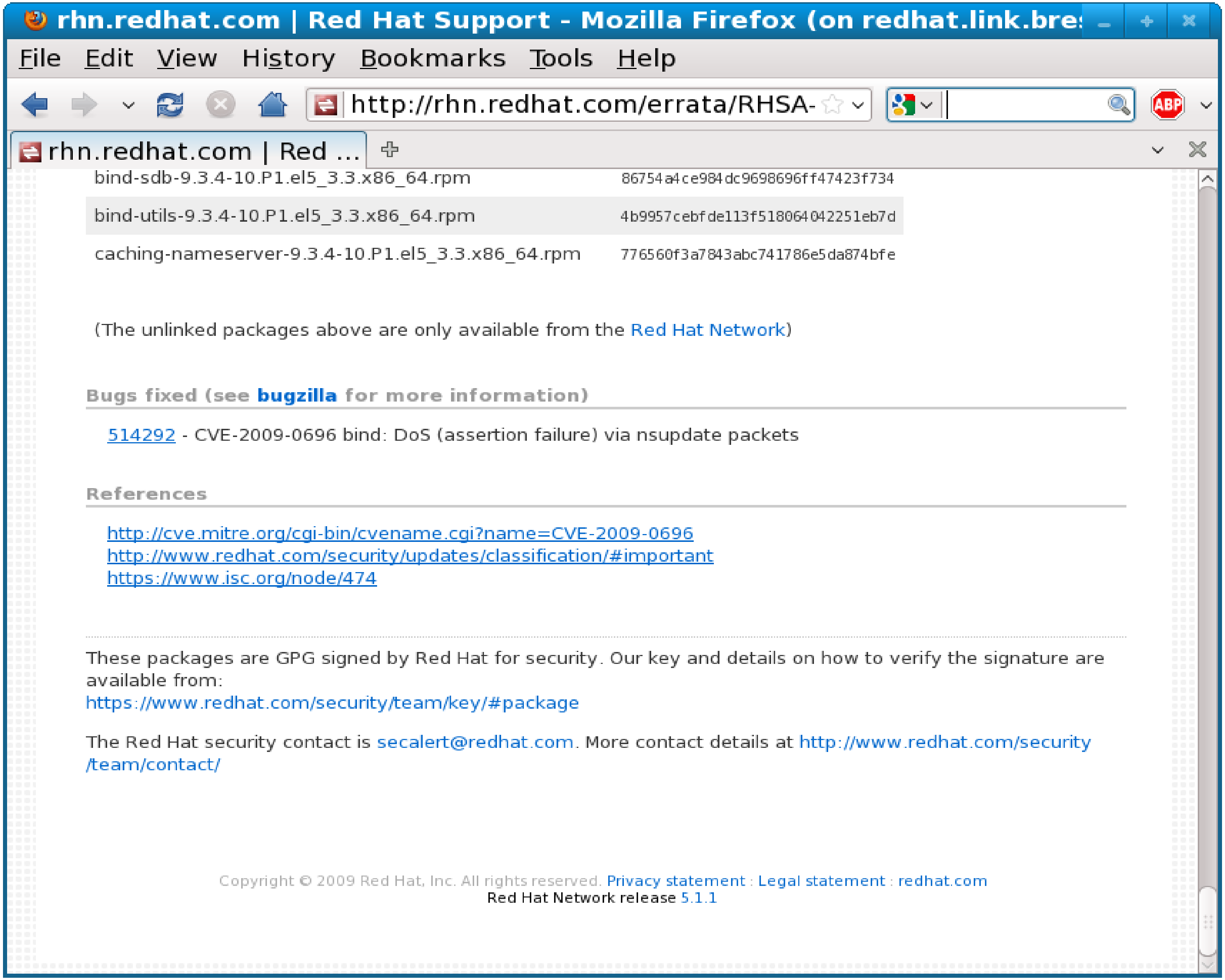
IA-32:

bind-chroot-9.3.4-10.P1.el5_3.3.i386.rpm	8aa7c2a7eeca72ce6af1826dbf693cbb
bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm	0cdece16263b7ed59d19e03a6bf9c58c
bind-libbind-devel-9.3.4-10.P1.el5_3.3.i386.rpm	4c9cfaa3681c8163d18b4ba0bf0e587f
caching-nameserver-9.3.4-10.P1.el5_3.3.i386.rpm	89b6bf69d881683ab64b69703b156ad2

x86_64:

bind-chroot-9.3.4-10.P1.el5_3.3.x86_64.rpm	94c2fcfd37bd404e04aaac40ce46bb71
bind-devel-9.3.4-10.P1.el5_3.3.i386.rpm	0cdece16263b7ed59d19e03a6bf9c58c
bind-devel-9.3.4-10.P1.el5_3.3.x86_64.rpm	610e77b48aa6c005c173a5a0d650bf18
bind-libbind-devel-9.3.4-10.P1.el5_3.3.i386.rpm	4c9cfaa3681c8163d18b4ba0bf0e587f
bind-libbind-devel-9.3.4-10.P1.el5_3.3.x86_64.rpm	a691ff311d9bad5968b2b12f838fefde
caching-nameserver-9.3.4-10.P1.el5_3.3.x86_64.rpm	776560f3a7843abc741786e5da874bfe

Bugs Fixed


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bre:
File Edit View History Bookmarks Tools Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...

bind-sdb-9.3.4-10.P1.el5_3.3.x86_64.rpm	86754a4ce984dc9698696ff47423f734
bind-utils-9.3.4-10.P1.el5_3.3.x86_64.rpm	4b9957cebfde113f518064042251eb7d
caching-nameserver-9.3.4-10.P1.el5_3.3.x86_64.rpm	776560f3a7843abc741786e5da874bfe

(The unlinked packages above are only available from the Red Hat Network)

Bugs fixed (see bugzilla for more information)

514292 - CVE-2009-0696 bind: DoS (assertion failure) via nsupdate packets

References

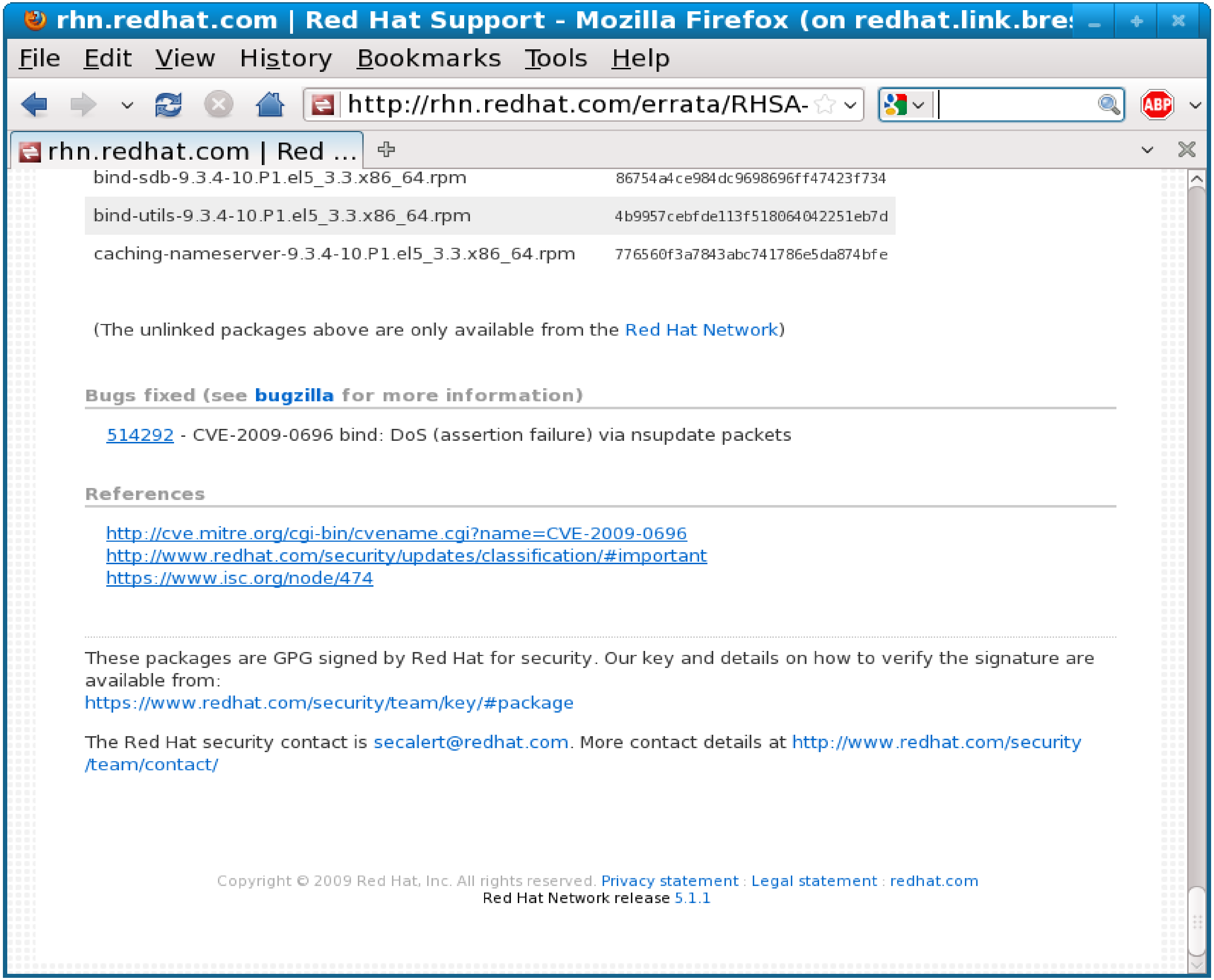
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696
http://www.redhat.com/security/updates/classification/#important
https://www.isc.org/node/474

These packages are GPG signed by Red Hat for security. Our key and details on how to verify the signature are available from:
https://www.redhat.com/security/team/key/#package

The Red Hat security contact is secalert@redhat.com. More contact details at http://www.redhat.com/security/team/contact/

Red Hat Network release 5.1.1

References


rhn.redhat.com | Red Hat Support - Mozilla Firefox (on redhat.link.bre:
File
Edit
View
History
Bookmarks
Tools
Help
http://rhn.redhat.com/errata/RHSA-
rhn.redhat.com | Red ...

bind-sdb-9.3.4-10.P1.el5_3.3.x86_64.rpm	86754a4ce984dc9698696ff47423f734
bind-utils-9.3.4-10.P1.el5_3.3.x86_64.rpm	4b9957cebfde113f518064042251eb7d
caching-nameserver-9.3.4-10.P1.el5_3.3.x86_64.rpm	776560f3a7843abc741786e5da874bfe

(The unlinked packages above are only available from the Red Hat Network)

Bugs fixed (see bugzilla for more information)

514292 - CVE-2009-0696 bind: DoS (assertion failure) via nsupdate packets

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696
http://www.redhat.com/security/updates/classification/#important
https://www.isc.org/node/474

These packages are GPG signed by Red Hat for security. Our key and details on how to verify the signature are available from:
https://www.redhat.com/security/team/key/#package

The Red Hat security contact is secalert@redhat.com. More contact details at http://www.redhat.com/security/team/contact/

Red Hat Network release 5.1.1

Mining for CVE data

What happens if I want information on a specific CVE id?

Old Way

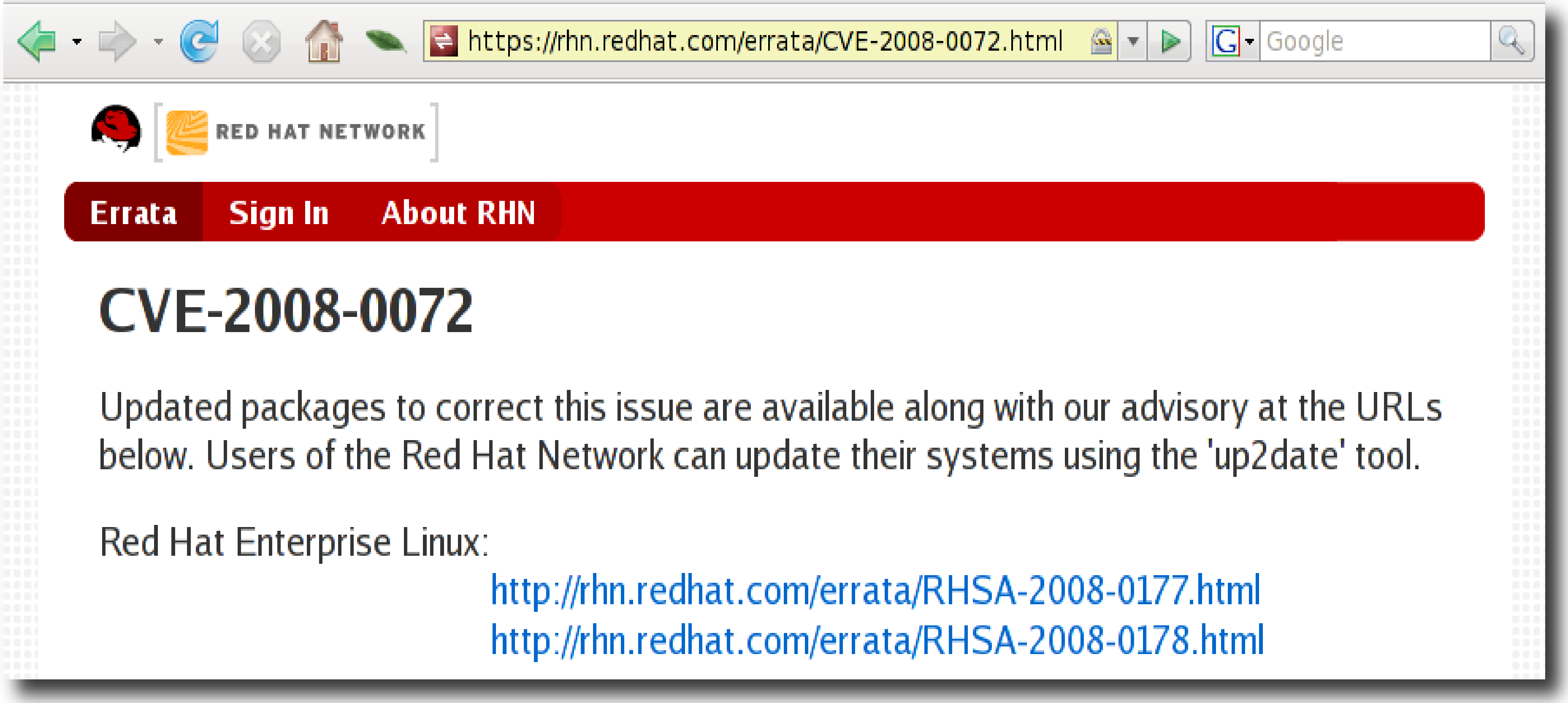
Our previous instructions were quite manual

Multiple locations had to be checked

Does an issue affect Red Hat?

Get the CVE name and use RHN

see if we've issued an update already

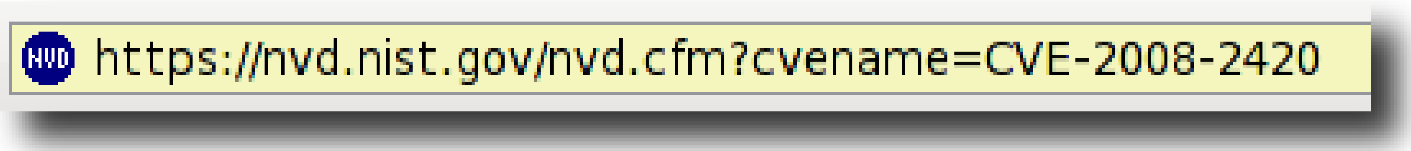


CVE-2008-0072

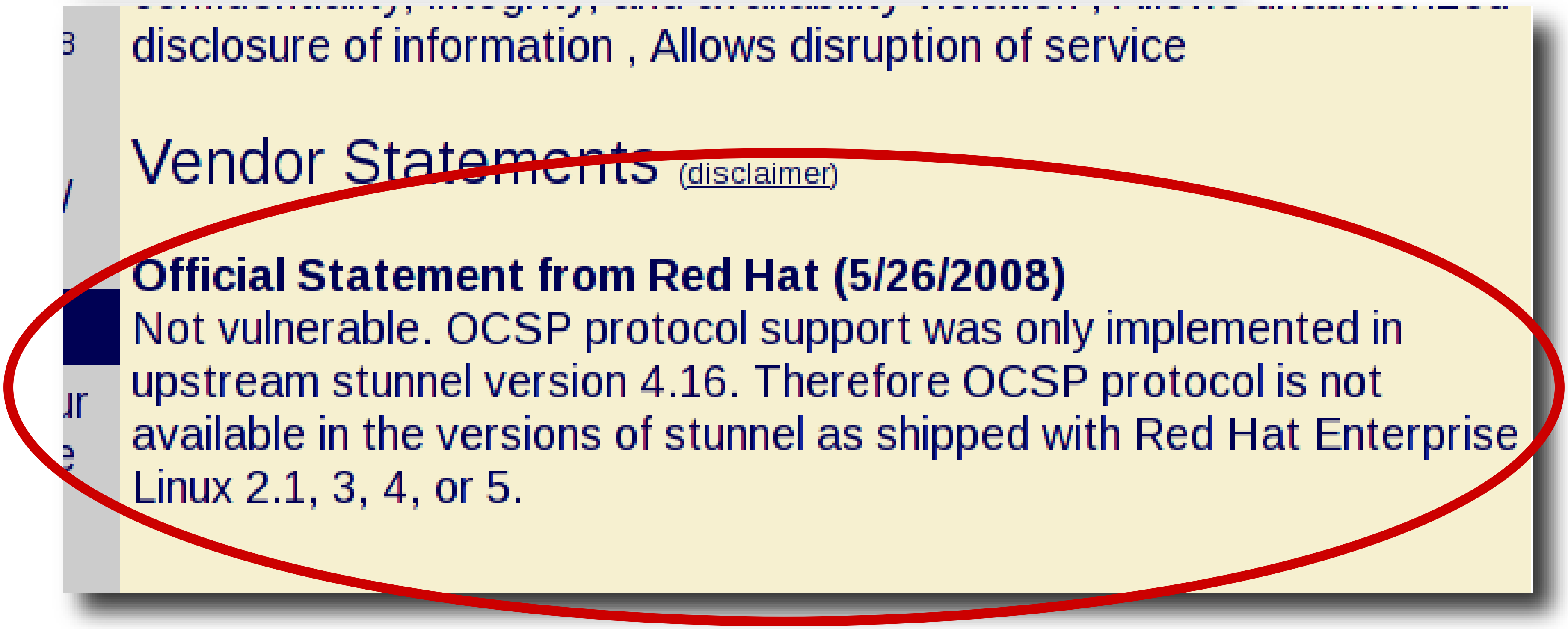
Updated packages to correct this issue are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool.

Red Hat Enterprise Linux:
http://rhn.redhat.com/errata/RHSA-2008-0177.html
http://rhn.redhat.com/errata/RHSA-2008-0178.html

Perhaps it doesn't affect us, try NVD



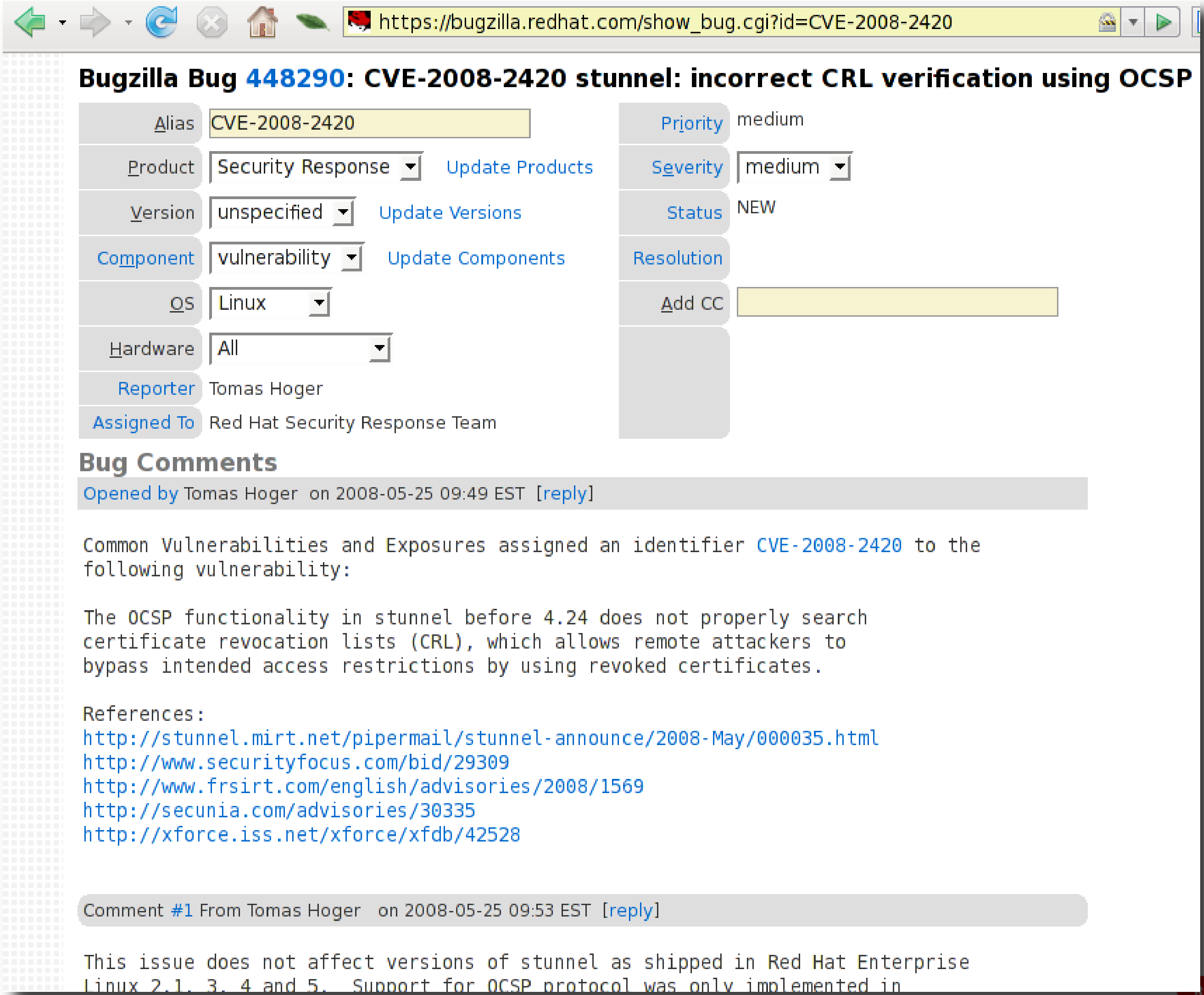
https://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2420



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.



https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2008-2420

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]

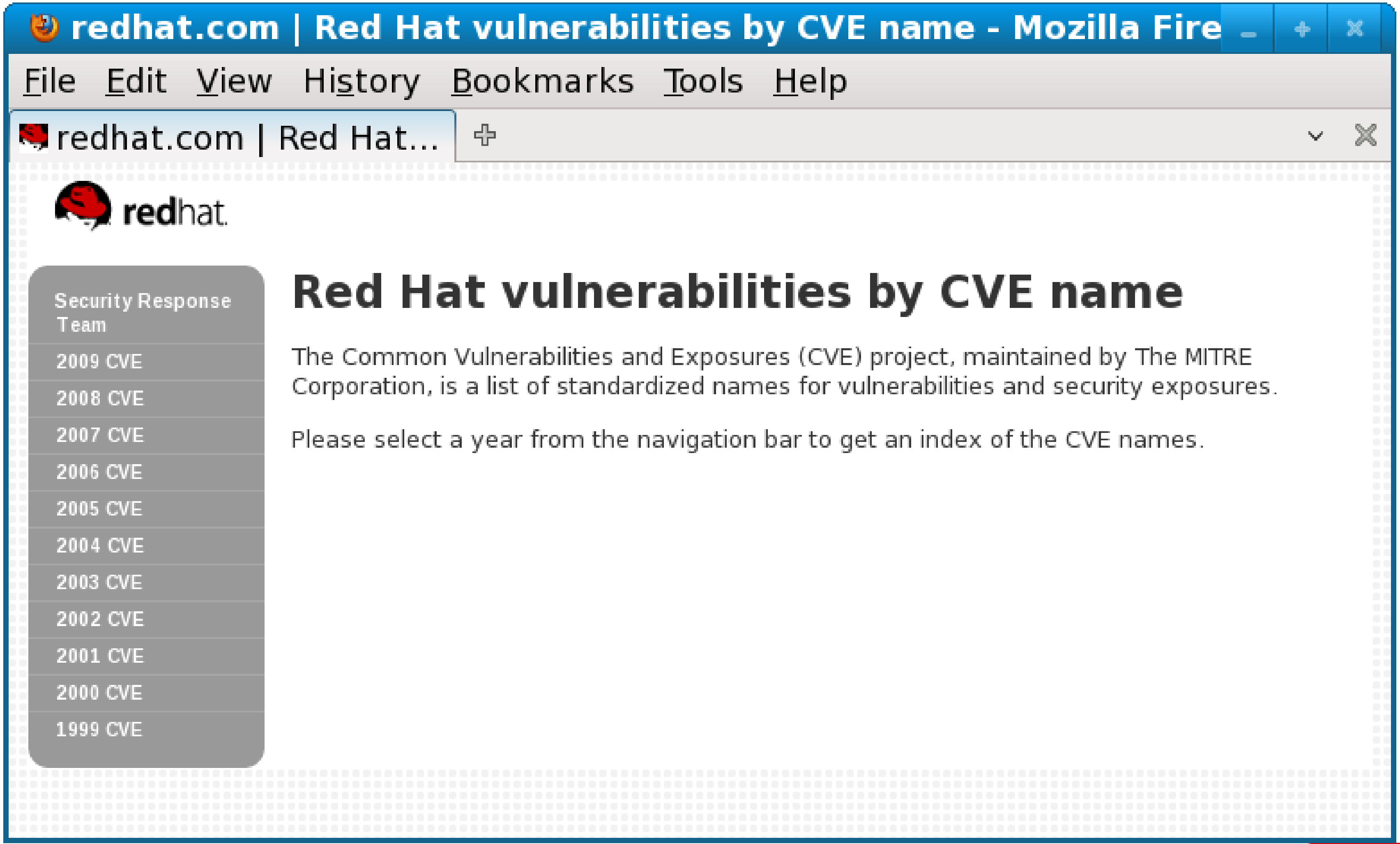
```
Common Vulnerabilities and Exposures assigned an identifier CVE-2008-2420 to the
following vulnerability:

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
```

New Way

http://www.redhat.com/security/data/cve


redhat.com | Red Hat vulnerabilities by CVE name - Mozilla Fire
File Edit View History Bookmarks Tools Help
redhat.com | Red Hat...
redhat.

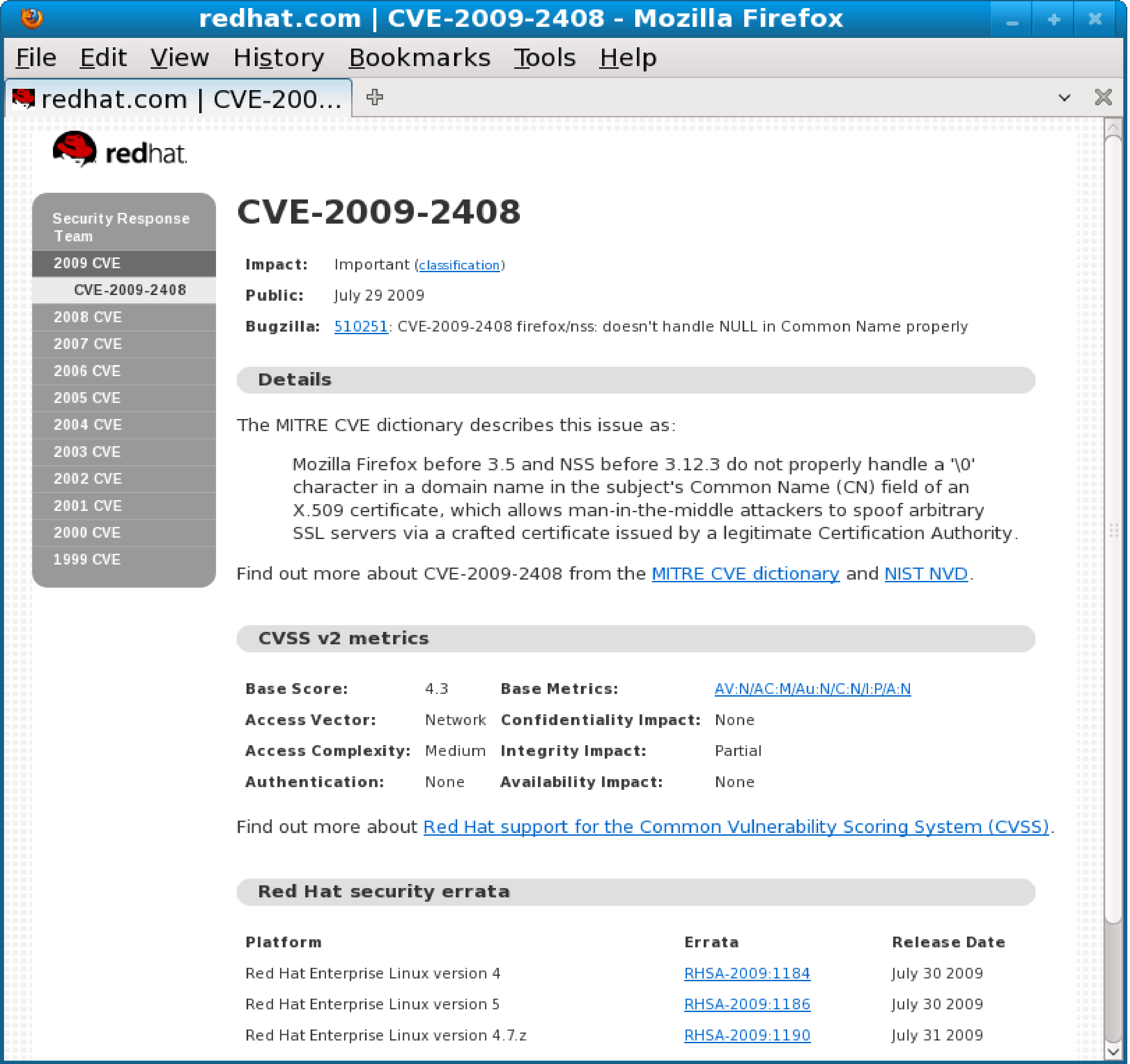
Security Response Team

- 2009 CVE
- 2008 CVE
- 2007 CVE
- 2006 CVE
- 2005 CVE
- 2004 CVE
- 2003 CVE
- 2002 CVE
- 2001 CVE
- 2000 CVE
- 1999 CVE

Red Hat vulnerabilities by CVE name

The Common Vulnerabilities and Exposures (CVE) project, maintained by The MITRE Corporation, is a list of standardized names for vulnerabilities and security exposures.

Please select a year from the navigation bar to get an index of the CVE names.



CVE-2009-2408

Impact:	Important (classification)
Public:	July 29 2009
Bugzilla:	510251: CVE-2009-2408 firefox/nss: doesn't handle NULL in Common Name properly

Details

The MITRE CVE dictionary describes this issue as:

> Mozilla Firefox before 3.5 and NSS before 3.12.3 do not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.

Find out more about CVE-2009-2408 from the MITRE CVE dictionary and NIST NVD.

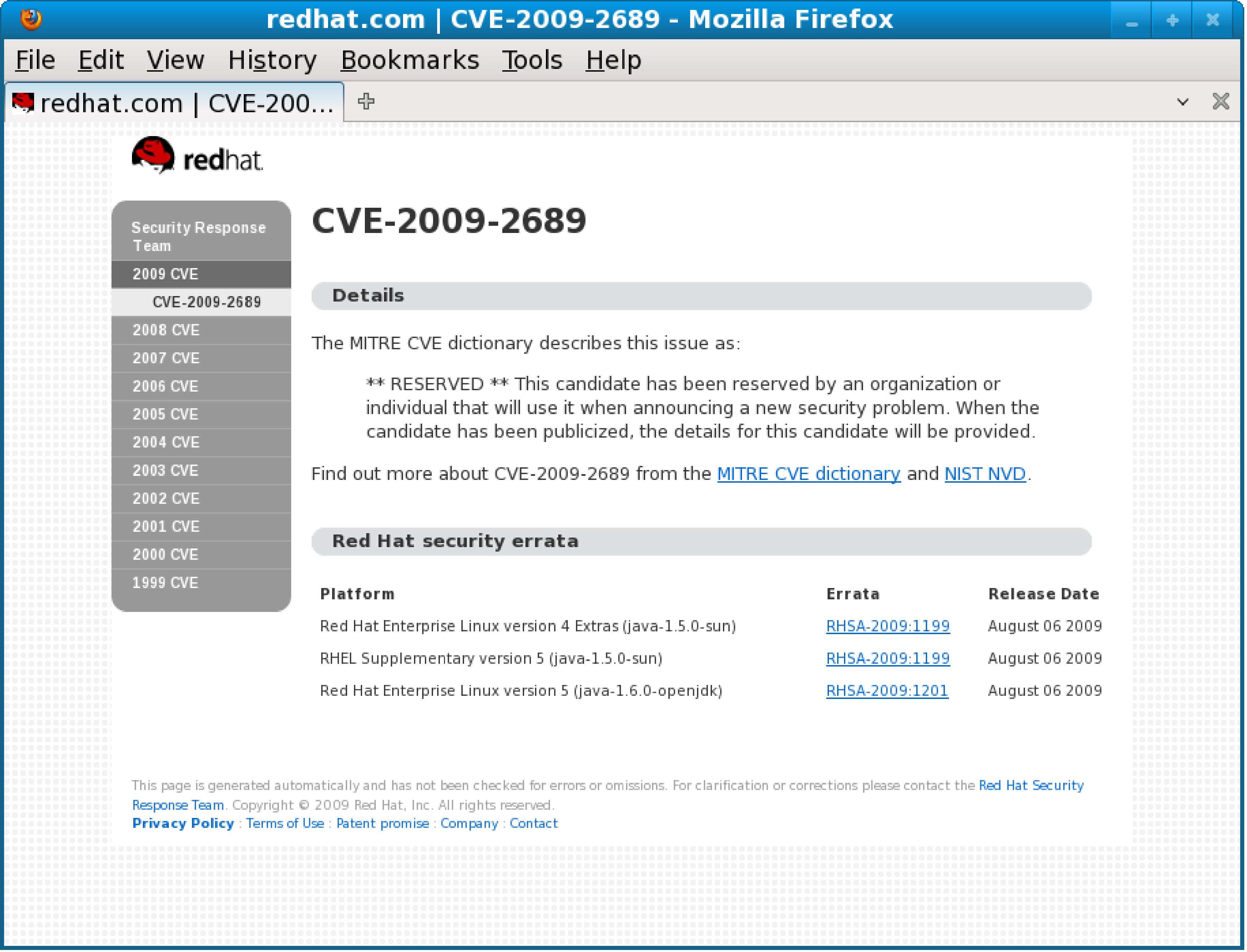
CVSS v2 metrics

Base Score:	4.3	**Base Metrics:**	AV:N/AC:M/Au:N/C:N/I:P/A:N
Access Vector:	Network	**Confidentiality Impact:**	None
Access Complexity:	Medium	**Integrity Impact:**	Partial
Authentication:	None	**Availability Impact:**	None

Find out more about Red Hat support for the Common Vulnerability Scoring System (CVSS).

Red Hat security errata

Platform	Errata	Release Date
Red Hat Enterprise Linux version 4	RHSA-2009:1184	July 30 2009
Red Hat Enterprise Linux version 5	RHSA-2009:1186	July 30 2009
Red Hat Enterprise Linux version 4.7.z	RHSA-2009:1190	July 31 2009



CVE-2009-2689

Details

The MITRE CVE dictionary describes this issue as:

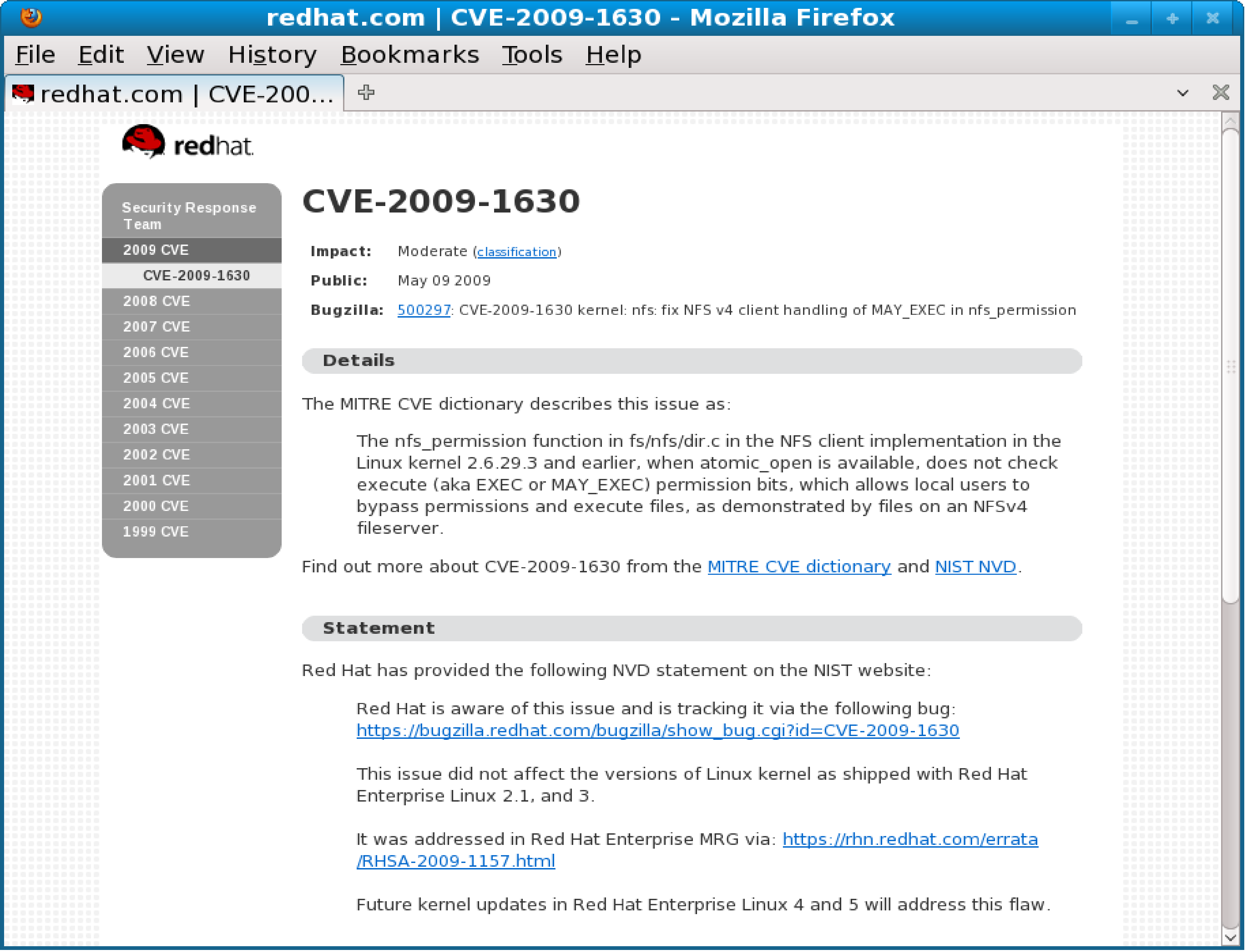
> ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

Find out more about CVE-2009-2689 from the MITRE CVE dictionary and NIST NVD.

Red Hat security errata

Platform	Errata	Release Date
Red Hat Enterprise Linux version 4 Extras (java-1.5.0-sun)	RHSA-2009:1199	August 06 2009
RHEL Supplementary version 5 (java-1.5.0-sun)	RHSA-2009:1199	August 06 2009
Red Hat Enterprise Linux version 5 (java-1.6.0-openjdk)	RHSA-2009:1201	August 06 2009

This page is generated automatically and has not been checked for errors or omissions. For clarification or corrections please contact the Red Hat Security Response Team. Copyright © 2009 Red Hat, Inc. All rights reserved.
Privacy Policy : Terms of Use : Patent promise : Company : Contact



CVE-2009-1630

Impact:	Moderate (classification)
Public:	May 09 2009
Bugzilla:	500297: CVE-2009-1630 kernel: nfs: fix NFS v4 client handling of MAY_EXEC in nfs_permission

Details

The MITRE CVE dictionary describes this issue as:

> The nfs_permission function in fs/nfs/dir.c in the NFS client implementation in the Linux kernel 2.6.29.3 and earlier, when atomic_open is available, does not check execute (aka EXEC or MAY_EXEC) permission bits, which allows local users to bypass permissions and execute files, as demonstrated by files on an NFSv4 fileserver.

Find out more about CVE-2009-1630 from the MITRE CVE dictionary and NIST NVD.

Statement

Red Hat has provided the following NVD statement on the NIST website:

> Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=CVE-2009-1630
>
> This issue did not affect the versions of Linux kernel as shipped with Red Hat Enterprise Linux 2.1, and 3.
>
> It was addressed in Red Hat Enterprise MRG via: https://rhn.redhat.com/errata/RHSA-2009-1157.html
>
> Future kernel updates in Red Hat Enterprise Linux 4 and 5 will address this flaw.

Passive Notification

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

From the web https://rhn.redhat.com/errata/

RSS feed

QUESTIONS?

TELL US WHAT YOU THINK:
REDHAT.COM/SUMMIT-SURVEY