JBoss WORLD
CHICAGO 2009

FOLLOW US:

TWITTER.COM/REDHATSUMMIT

TWEET ABOUT US:

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

presented by

JBoss WORLD CHICAGO 2009

Security Assurance With JBoss Enterprise Application Platform (EAP)

Anil Saldhana
Lead JBoss Security Architect, Red Hat
September 3, 2009

presented by

Agenda

- Introduction to assurance with EAP
- Configuration
- Certification
- Response Process
- Q&A

Introduction to assurance with EAP

- Three areas to consider in assurance
  - Configuration
  - Certification
  - Response Mechanism

Configuration

- Configuration is secure by default
- Reasonable defaults are applied
  - JMX invokers are all secure.
  - Admin consoles need configuration (no default use).
- Facilities to eliminate clear text password in files
  - Datasource Passwords
  - LoginModule Passwords
  - Tomcat Connector Passwords etc

Certification

- JBoss EAP 4.3 is Common Criteria Certified.
  - Evaluation Assurance Level 2+
    - EAL- numerical rating describing depth/rigor of evaluation
  - ISO/ISEC 15408 International Standard
  - Certified by NIAP (Natl Infor. Assurance Parnership)
    - US Government Initiative
  - Independent Evaluating Laboratory
    - ATSec

Certification

- JBoss EAP 4.3 is Common Criteria Certified.
- What is evaluated at varying depths by independent external security evaluators :
  - Design Documents
  - Source Code
  - Test Plan
  - Test Suite
  - Release Process
  - Response Process etc.

Certification

- JBoss EAP 4.3 is Common Criteria Certified.
- Common Criteria Certified Configuration
  - Outlined in the configuration guide
  - Two modes:
    - Java Security Manager Enabled. (Preferred/Suggested)
    - Java Security Manager Disabled.

Response Process

- Handled mainly by the Red Hat Security Response Team
- Handle 85 released RH product versions (Nov.2008)
- Handle, triage and investigate about 50 vulnerabilities per month.
- Staff in around 6 countries worldwide.
- 2008: Triaged 6 vulnerabilities per week.
  - *Triage involves separate issues that are important, examine the products/versions affected etc.*

Response Process – Red Hat Response Team

- Accountable for vulnerabilities that affect all RH products
  - 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

Response Process – Release Policy

- Critical Vulnerabilities
  - *Pushed immediately or when embargo lifted or QE finished.*
  - *Any time of day/week – holidays/weekends.*
- Important Vulnerabilities
  - *Reasonable time and day (M-Thu)*
- Moderate or Low Vulnerabilities
  - *Next update release or wait for other issues affecting the same package.*

low
moderate
important
critical
least impact
most impact

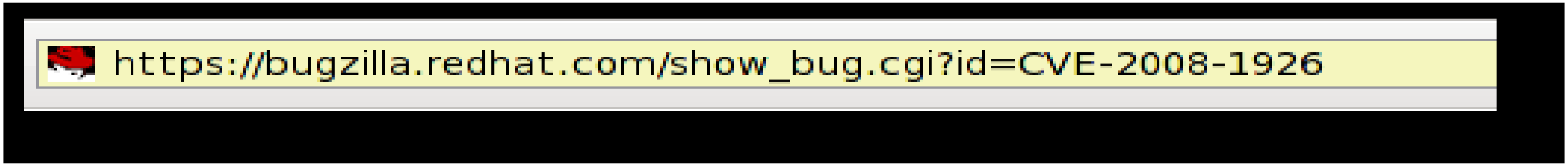
Response Process – Cycle – Part 1

- Vulnerability reported, learned...
- Triage
- Construct the Security Errata
  - *Credit the reporters*
  - *Collate packages*
- QE

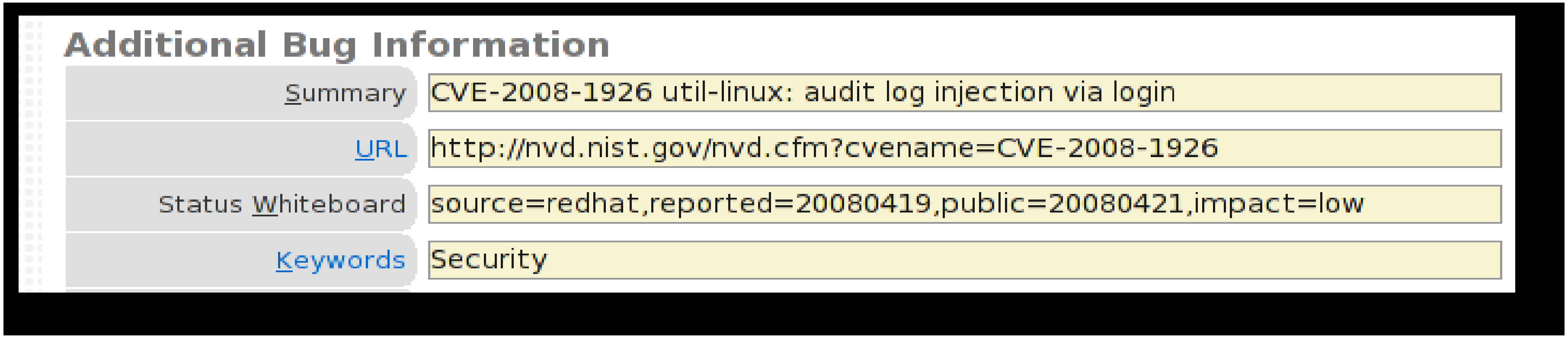
Response Process – Cycle – Part 2

- Release
- Pick up updated packages from Red Hat Network (RHN) Channels
  - *Email alerts in RHN, enterprise-watch-list@redhat.com, rhsa-announce@redhat.com*
  - *Web : https://rhn.redhat.com/errata/*

Response Process – Finding Vulnerability

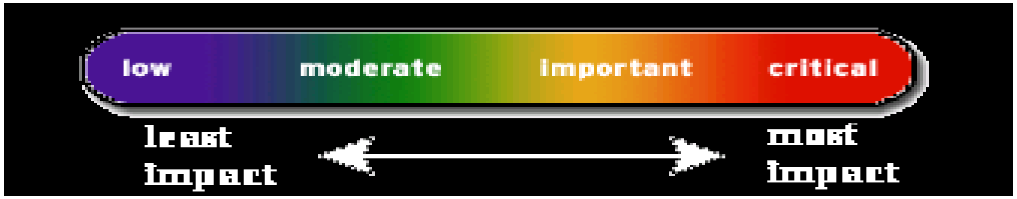


https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2008-1926

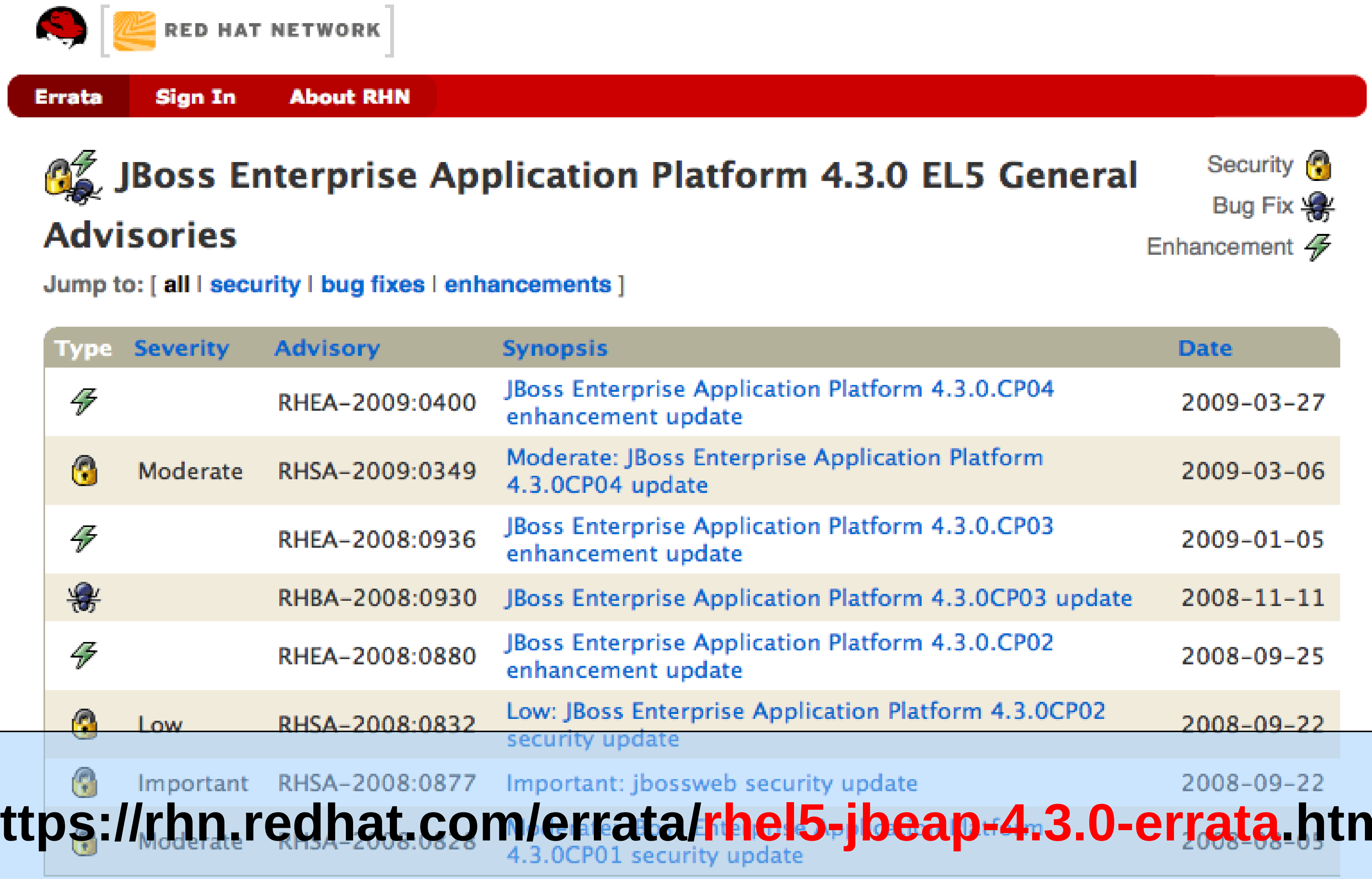


Additional Bug Information

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=20080421,impact=low
Keywords	Security



RHN: Trackable History Of Security Advisories



JBoss Enterprise Application Platform 4.3.0 EL5 General Advisories

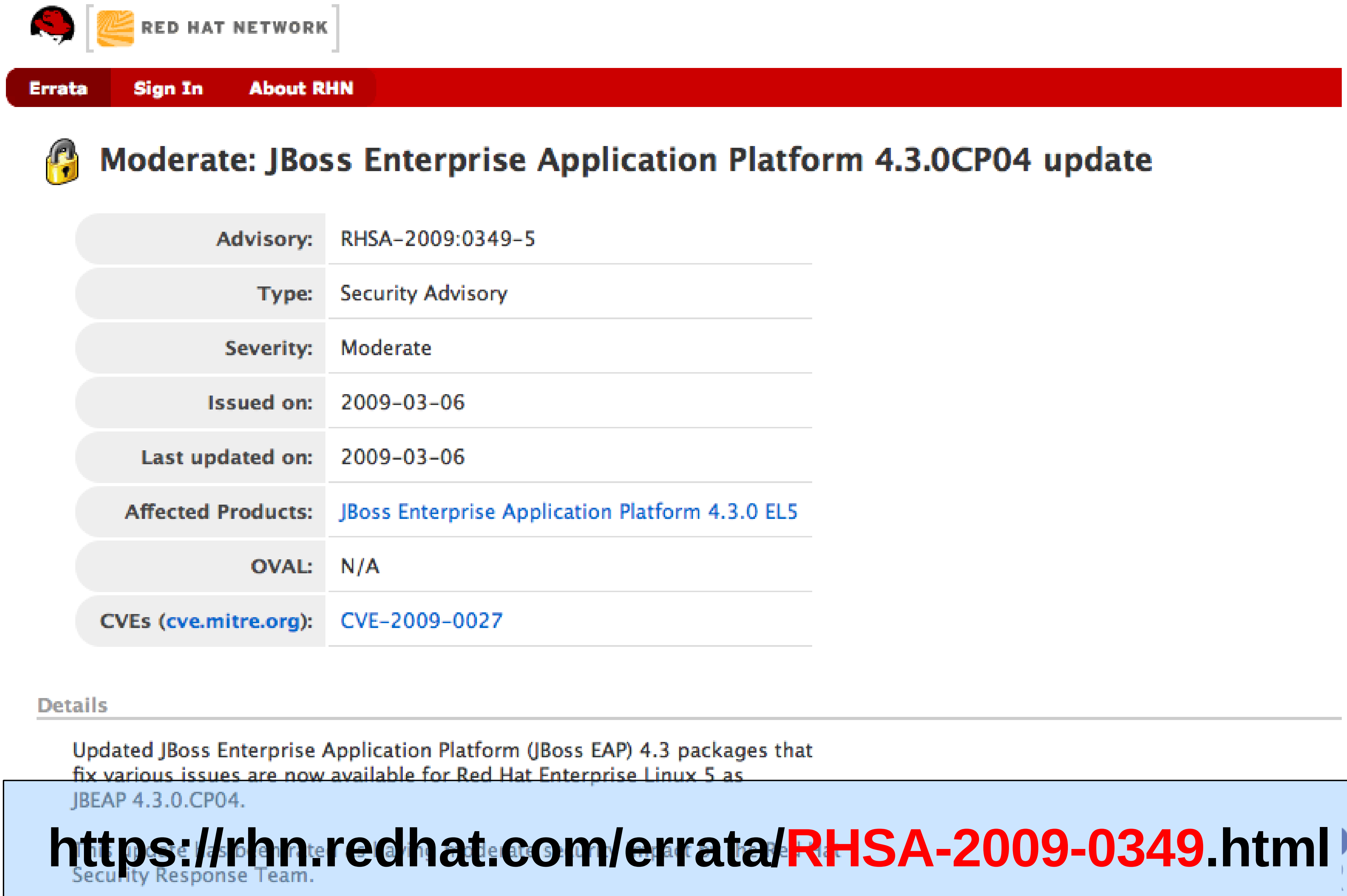
Security 🔒
Bug Fix 🐞
Enhancement ⚡

Jump to: [all | security | bug fixes | enhancements]

Type	Severity	Advisory	Synopsis	Date
⚡		RHEA-2009:0400	JBoss Enterprise Application Platform 4.3.0.CP04 enhancement update	2009-03-27
🔒	Moderate	RHSA-2009:0349	Moderate: JBoss Enterprise Application Platform 4.3.0CP04 update	2009-03-06
⚡		RHEA-2008:0936	JBoss Enterprise Application Platform 4.3.0.CP03 enhancement update	2009-01-05
🐞		RHBA-2008:0930	JBoss Enterprise Application Platform 4.3.0CP03 update	2008-11-11
⚡		RHEA-2008:0880	JBoss Enterprise Application Platform 4.3.0.CP02 enhancement update	2008-09-25
🔒	Low	RHSA-2008:0832	Low: JBoss Enterprise Application Platform 4.3.0CP02 security update	2008-09-22
🔒	Important	RHSA-2008:0877	Important: jbossweb security update	2008-09-22
🔒	Moderate	RHSA-2008:0828	Moderate: JBoss Enterprise Application Platform 4.3.0CP01 security update	2008-08-05

https://rhn.redhat.com/errata/rhel5-jbeap-4.3.0-errata.html

Security Fixes Are Bundled In Advisories



Moderate: JBoss Enterprise Application Platform 4.3.0CP04 update

Advisory:	RHSA-2009:0349-5
Type:	Security Advisory
Severity:	Moderate
Issued on:	2009-03-06
Last updated on:	2009-03-06
Affected Products:	JBoss Enterprise Application Platform 4.3.0 EL5
OVAL:	N/A
CVEs (cve.mitre.org):	CVE-2009-0027

Details

Updated JBoss Enterprise Application Platform (JBoss EAP) 4.3 packages that fix various issues are now available for Red Hat Enterprise Linux 5 as JBEAP 4.3.0.CP04.

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

https://rhn.redhat.com/errata/RHSA-2009-0349.html

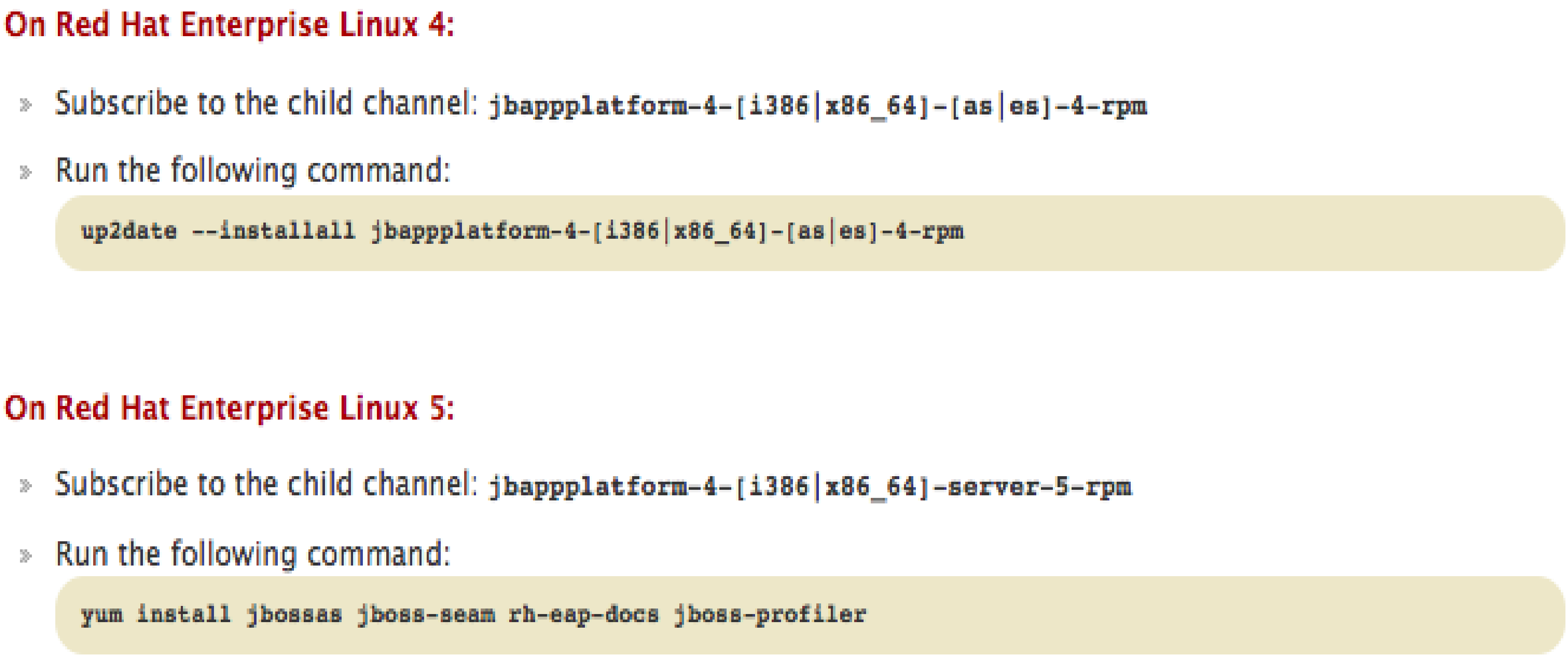
How To Get Notified

RHN & JBoss Customer Support Portal will notify you of updates needed to packages installed on your systems

- By email (if you enable it)
- By up2date/pup (RHEL)
- By logging in
- Filters alert to those that affect your installation (RHN)
- Subscribing to Advisory Lists
    - jboss-watch-list@redhat.com
    - rhsa-announce@redhat.com
    - you can even limit by severity
- From the web: https://rhn.redhat.com/errata/
- RSS feed

Manage a JBoss installation via RHN

Example: JBoss Enterprise Application Platform



On Red Hat Enterprise Linux 4:

- Subscribe to the child channel: `jbappplatform-4-[i386|x86_64]-[as|es]-4-rpm`
- Run the following command:

```
up2date --installall jbappplatform-4-[i386|x86_64]-[as|es]-4-rpm
```

On Red Hat Enterprise Linux 5:

- Subscribe to the child channel: `jbappplatform-4-[i386|x86_64]-server-5-rpm`
- Run the following command:

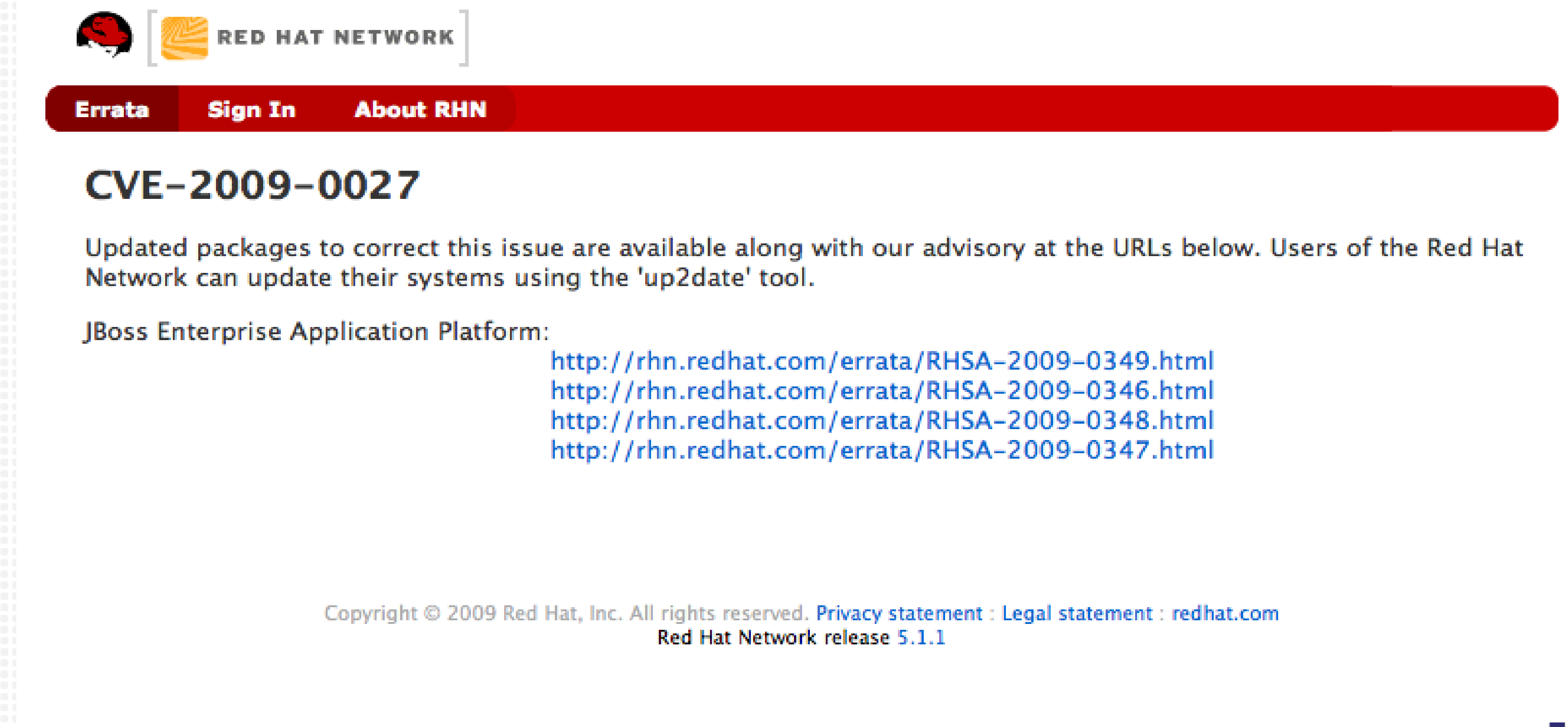
```
yum install jbossas jboss-seam rh-eap-docs jboss-profiler
```

Does an issue affect JBoss?

Example: JBoss Enterprise Application Platform on RHEL

Use the CVE name to verify RHN updates for a specific issue:

http://rhn.redhat.com/errata/CVE-2009-0027.html



CVE-2009-0027

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.

JBoss Enterprise Application Platform:

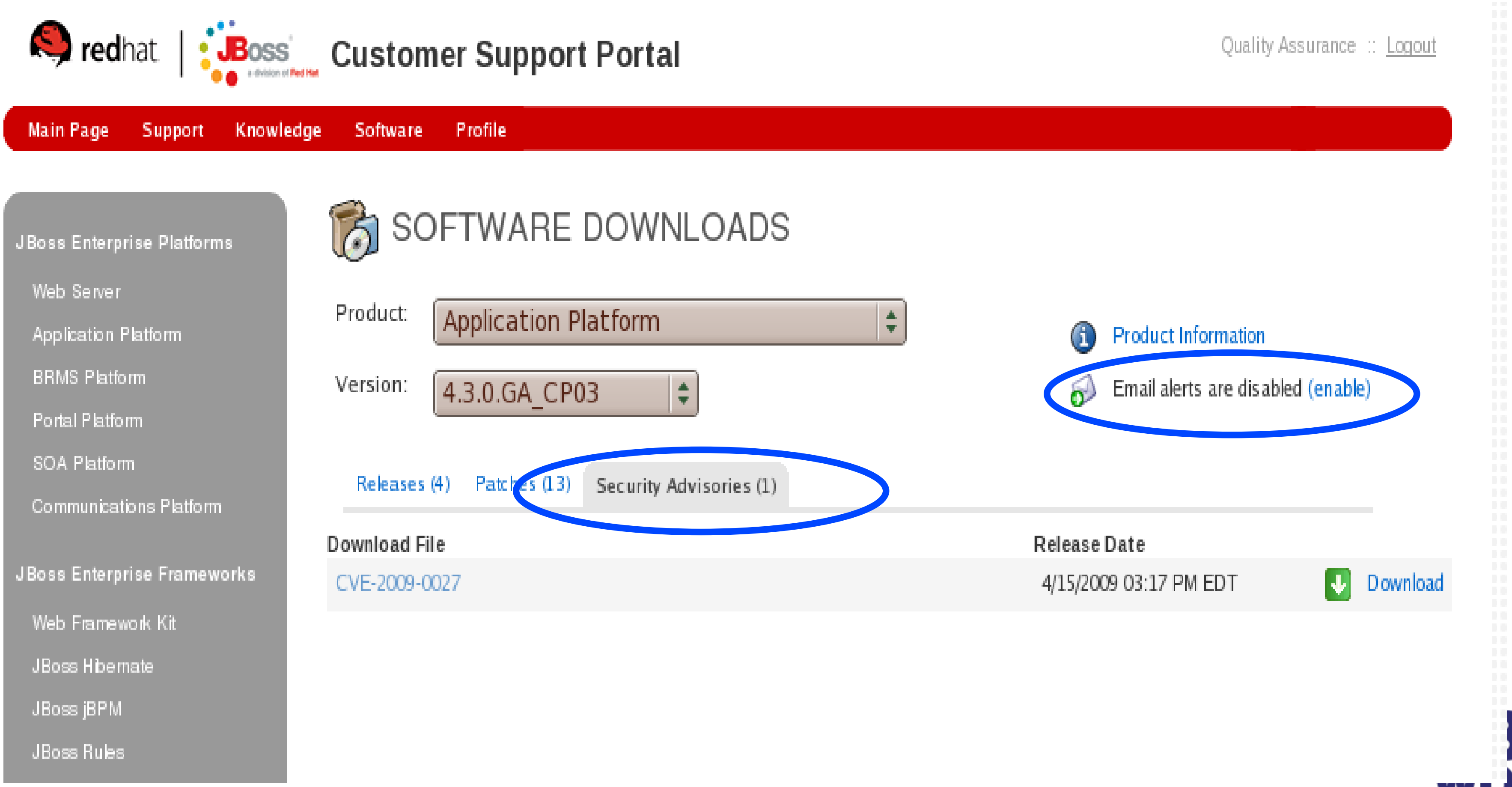
http://rhn.redhat.com/errata/RHSA-2009-0349.html
http://rhn.redhat.com/errata/RHSA-2009-0346.html
http://rhn.redhat.com/errata/RHSA-2009-0348.html
http://rhn.redhat.com/errata/RHSA-2009-0347.html

Copyright © 2009 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
Red Hat Network release 5.1.1

Does an issue affect JBoss?

Example: JBoss Enterprise Application Platform on other platforms

Use the JBoss Customer Support Portal (CSP) for updates to non-RHEL platforms (e.g. Windows, Unix, other Linux)



SOFTWARE DOWNLOADS

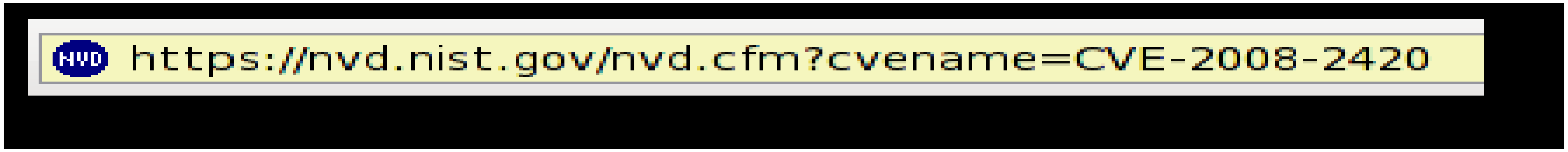
Product: Application Platform

Version: 4.3.0.GA_CP03

Email alerts are disabled (enable)

Download File	Release Date	
CVE-2009-0027	4/15/2009 03:17 PM EDT	Download

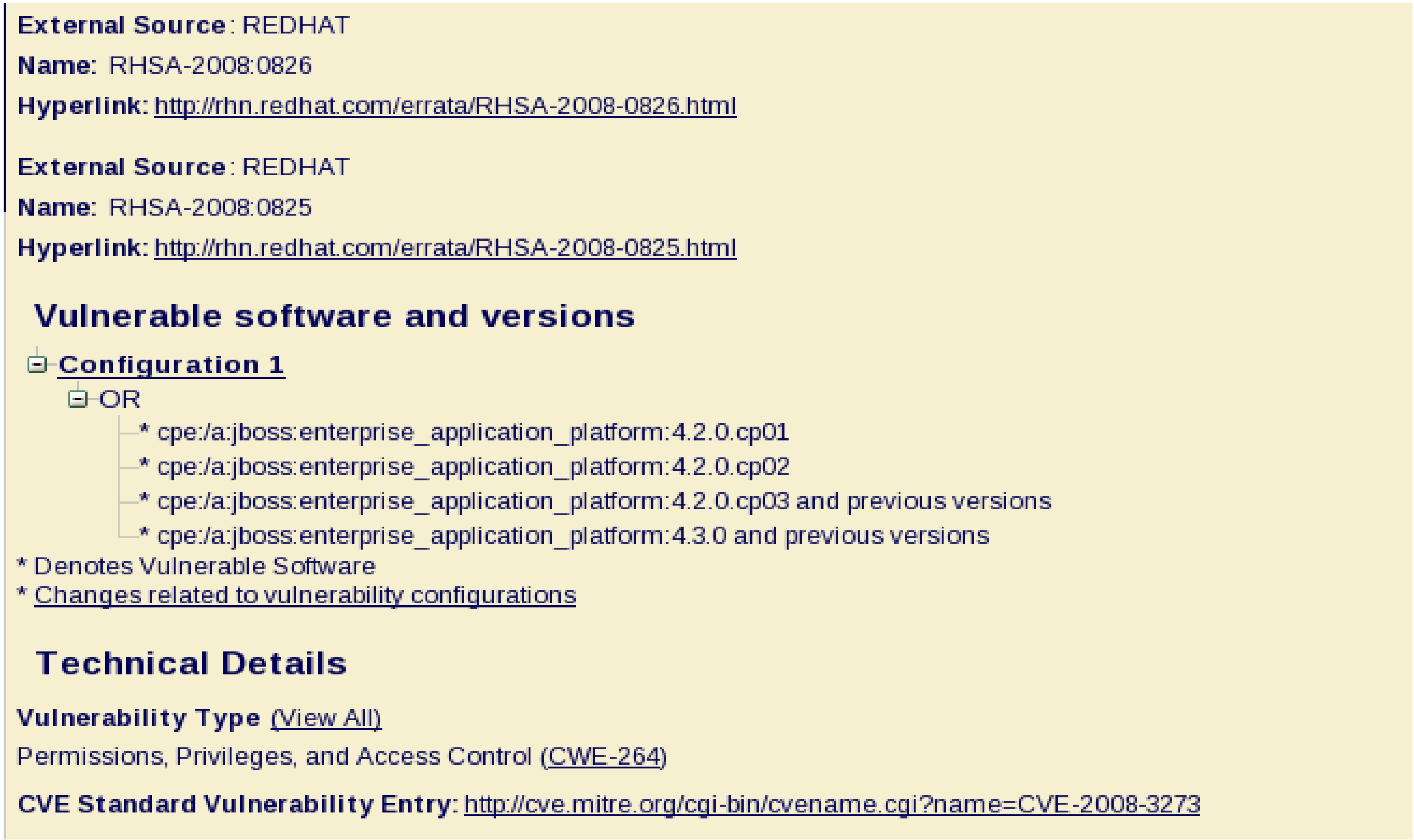
NVD (National Vulnerability Database)



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

To query the CVE name with NVD, use:

http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3273



External Source: REDHAT

Name: RHSA-2008:0826

Hyperlink: http://rhn.redhat.com/errata/RHSA-2008-0826.html

External Source: REDHAT

Name: RHSA-2008:0825

Hyperlink: http://rhn.redhat.com/errata/RHSA-2008-0825.html

Vulnerable software and versions

Configuration 1

OR

- * cpe:/a:jboss:enterprise_application_platform:4.2.0.cp01
- * cpe:/a:jboss:enterprise_application_platform:4.2.0.cp02
- * cpe:/a:jboss:enterprise_application_platform:4.2.0.cp03 and previous versions
- * cpe:/a:jboss:enterprise_application_platform:4.3.0 and previous versions

* Denotes Vulnerable Software

* Changes related to vulnerability configurations

Technical Details

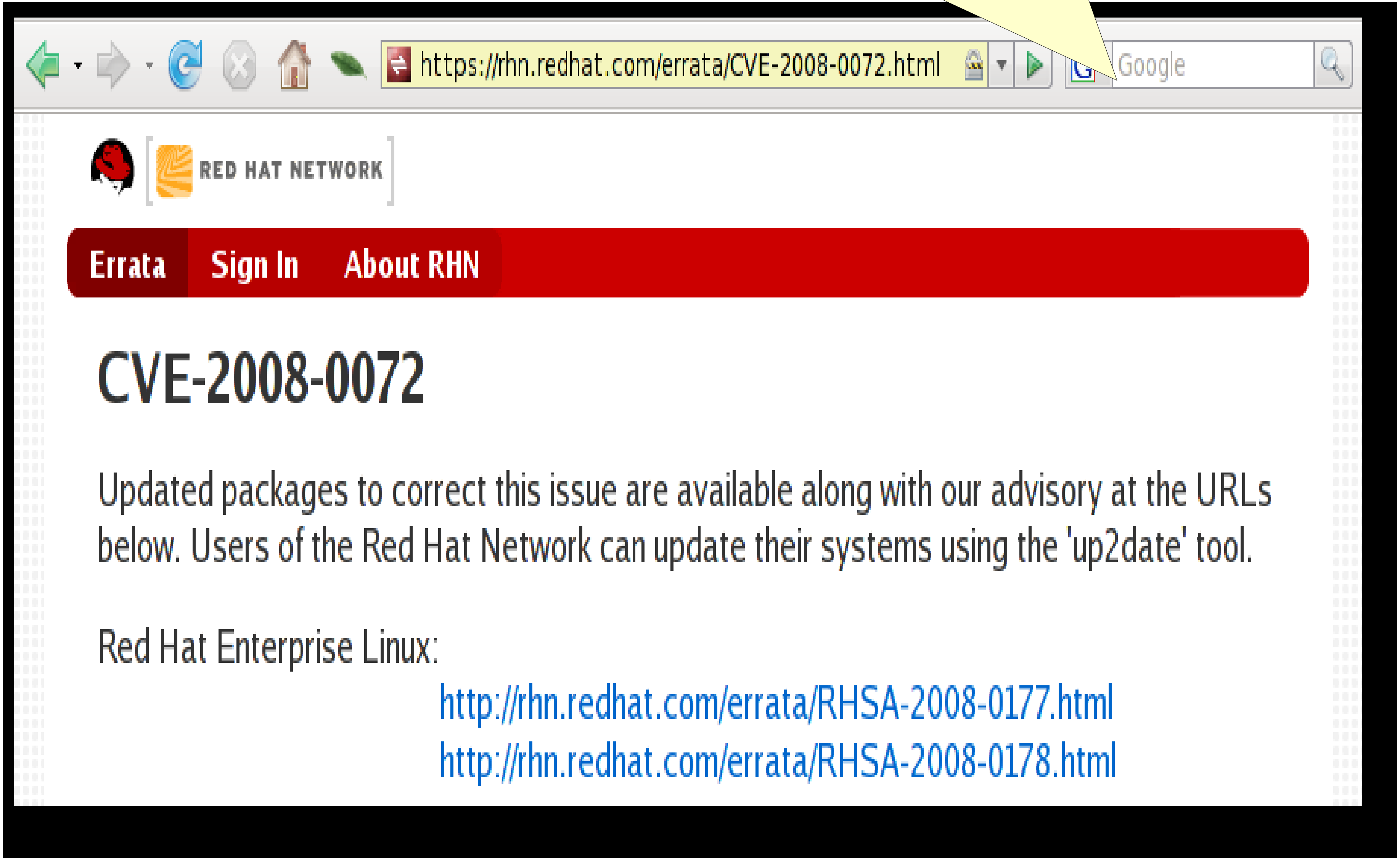
Vulnerability Type (View All)

Permissions, Privileges, and Access Control (CWE-264)

CVE Standard Vulnerability Entry: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3273

Response Process – CVE

Common Vulnerability Enumeration is a dictionary of publicly known vulnerabilities.



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

How Do I Contact Red Hat Security Response?

secalert@redhat.com

Used to ask security vulnerability related questions

- Reporting new vulnerabilities
- Asking how we addressed various vulnerabilities
- Charter to respond within 3 business days

96%

secalert@redhat.com mails had first response within 1 business day (Feb 2008 - Mar 2009)

References

- Red Hat Security: http://www.redhat.com/security
- Anil's Blog: http://anil-identity.blogspot.com
- Mark Cox's Blog: http://www.awe.com/mark/blog

QUESTIONS?

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