OPEN SOURCE, RED HAT, AND SECURITY

RICK RING, SENIOR SOLUTION ARCHITECT, RED HAT GLOBAL SERVICES

ABSTRACT

Red Hat, the world's leading provider of open source solutions, is committed to utilizing the principles of open source to provide enterprise-level security to its customers. This paper reviews open source software development principles and process and how those lead to more secure software. It also evaluates Red Hat® Enterprise Linux® security in the real world.

WHY OPEN SOURCE?

Red Hat technology is open source, built in collaboration with a rapidly growing worldwide community. Open source software grants every user access to its source code, creating better software. It returns control to the customer. You can see the code, change it, learn from it. Bugs are found and fixed quickly. When everyone collaborates, the best technology wins. Not just within one company, but among an Internet-connected, worldwide community. New ideas and code travel the world in an instant. As a result, the open source model often builds higher quality, more secure, more easily integrated software. And at a vastly accelerated pace and frequently lower cost.

WHO IS DOING THE WORK?

When it comes to Linux, Red Hat is the largest contributor. The Linux Foundation keeps track of who is working on the Linux kernel and routinely publishes the information on its website[1].

The Linux kernel is a resource that is used by a large variety of companies; many will never participate in the development of the kernel. They are content with the software as it is and do not feel the need to help drive its development in any particular direction. But, as can be seen in Figure 1, an increasing number of companies are working toward the improvement of the kernel, and Red Hat is the top company contributor.

SECURITY IN OPEN SOURCE

In December 2004, Wired Magazine published a study of the bugs per lines of code in proprietary software versus the Linux kernel code, and found:

Bugs per 1,000 lines of code:

- 20–30 bugs in proprietary software (Carnegie Mellon University Cylab)
- 0.17 bugs in the Linux 2.6 kernel (Stanford University/Cover)
- The Department of Homeland Security did a similar study, and the following results were published in *InformationWeek* on January 7, 2008:

Bugs per 1,000 lines of code:

- One bug in proprietary software
- 0.127 bugs in the Linux 2.6 kernel
- 0.14 bugs in Apache
- 0.041 bugs in PostgreSQL
- Zero bugs in gcc

The claims of the open source community are being realized in the real world.

COMPANY NAME	NUMBER OF CHANGES	PERCENT OF TOTAL
None	11,594	13.9
Unknown	10,803	12.9
Red Hat	**9,351**	**11.2**
Novell	7,385	8.9
IBM	6,952	8.3
Intel	3,388	4.1
Linux Foundation	2,160	2.6
Consultant	2,055	2.5
SGI	1,649	2.0
MIPS Technologies	1,341	1.6
Oracle	1,122	1.3
MontaVista	1,010	1.2
Google	965	1.1
Linutronix	817	1.0
HP	765	0.9
NetApp	764	0.9
SWsoft	762	0.9
Renesas Technology	759	0.9
Freescale	730	0.9
Astaro	715	0.9
Academia	656	0.8
Cisco	442	0.5
Simtec	437	0.5
Linux Networx	434	0.5
QLogic	398	0.5
Fujitsu	389	0.5
Broadcom	385	0.5
Analog Devices	358	0.4
Mandriva	329	0.4
Mellanox	294	0.4
Snapgear	285	0.3

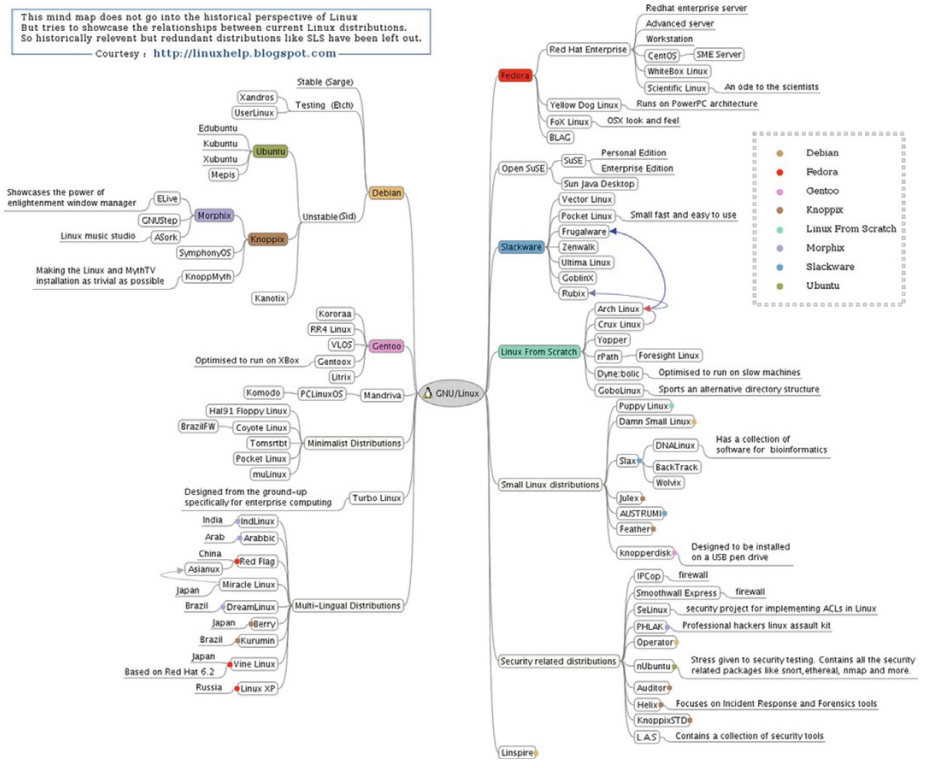
RED HAT AND FEDORA DEVELOPMENT

The core of the Linux operating system is the kernel. Development of the kernel is focused at kernel.org. The Linux kernel development process has been described as a benevolent dictatorship. Patches and enhancement are submitted for all parts of the Linux kernel by developers worldwide, thereby creating a borderless community. Vetting and integrating this diverse set of contributions falls to the approximately 80 subsystem maintainers who focus on and contribute to particular aspects of the kernel, such as file systems, memory management, or the system call interface.

Other components are built around projects designed to accomplish specific goals or solve specific problems. As someone has an innovative idea, a project is started and people join the team to develop the software. There are then various distribution projects where these individual projects coalesce into the different distributions.

Fedora® is a Red Hat-sponsored and community-supported open source project. It provides a public development platform and proving ground for new open source technologies. Technologies mature and are tested and integrated in the Fedora environment. Red Hat Enterprise Linux is distilled from the most mature and stable open source projects using the Fedora Project as a development and test platform. Fedora features that are proven mature and stable are incorporated into commercial, enterprise-ready Red Hat products. Figure 3 from **linuxhelp.blogspot.com/2006/04/mind-map-of-linux-distributions.html** shows the relationship of various distributions in the community.

THE RELATIONSHIP OF VARIOUS LINUX DISTRIBUTIONS



Red Hat takes the best technology pieces from Fedora distributions—those that are needed by enterprise customers—and packages them into Red Hat Enterprise Linux for a fully certified, enterprise-class operating platform.

There are several components in the process of producing Red Hat Enterprise Linux:

- Code review
- Security validation
- Version matching and validation
- Hardware testing and certification

This process produces a product that has been extensively reviewed, tested, and certified for enterprise use.

ONGOING SECURITY

Though reviewed, tested, and certified for enterprise use, experience has shown that almost no software is perfect—flaws or vulnerabilities may still be found. But, the open source development model provides a fast-innovating and reliable resource to bring forth the best software in the fastest time, including security fixes. As the ongoing management and remediation of flaws and vulnerabilities is just as important as the initial development process, Red Hat has a robust and open security program. Much of the following information is available at the Red Hat website[2].

SECURITY UPDATES

Red Hat releases errata to address bugs, provide enhancements, or to fix security vulnerabilities. With each erratum, Red Hat supplies an advisory to give details of the issues being fixed as well as how to obtain and install the required software packages. Links to the advisories for our products can be found at **www.redhat.com/security/updates/**.

VULNERABILITY REMEDIATION

As security vulnerabilities are discovered, the affected software must be updated in order to limit any potential security risks. If the software is part of a package within a Red Hat Enterprise Linux distribution that is currently supported, Red Hat is committed to releasing updated packages that fix the vulnerability as soon as possible.

Often, announcements about a given security exploit are accompanied with a patch, or source code that fixes the problem. This patch is then applied to the Red Hat Enterprise Linux package, tested by the Red Hat quality assurance team, and released as an errata update. If an announcement does not include a patch, a Red Hat developer works with the maintainer of the software to fix the problem. Once the problem is fixed, the package is tested and released as an errata update.

If an errata update is released for software used on your system, it is highly recommended that you update the affected packages as soon as possible to minimize the amount of time the system is potentially vulnerable.

NOTIFICATION OF ERRATA

Red Hat provides information about security flaws that affect Red Hat products and services in the form of Security Advisories. Advisories for all Red Hat products are published to a relevant Red Hat mailing list. The mailing lists are open for subscription to anyone and have publicly accessible archives.

For products serviced by the Red Hat Network systems management solution, Red Hat also provides advisories and update notifications via Red Hat Network.

To verify the source of this information, all advisories sent by email from Red Hat are digitally signed.

OFFICIAL STATEMENTS

Where a new public security vulnerability is under investigation, or where an issue does not affect Red Hat, Red Hat provides official vendor statements. These statements are available at the NIST National Vulnerability Database[3] and can be found by searching by CVE name, or as a complete downloadable file[4].

Red Hat advisories contain credits or acknowledgments where appropriate. We aim to include acknowledgments of companies or individuals that have reported issues to us in a responsible fashion.

SECURITY RESPONSE TEAM

Red Hat has a focused Security Response Team responsible for managing ongoing security of Red Hat-supported products. The Red Hat Security Response Team is responsible for ensuring that security issues found in Red Hat products and services are fully addressed.

The Red Hat Security Response Team mission is:

- Be a contact point for customers who have found security issues in Red Hat products or services and publish procedures for dealing with this contact.
- Track alerts and security issues within the community that may affect users of Red Hat products and services.
- Investigate and address security issues in supported products and services.
- Ensure timely security fixes for products.
- Ensure that customers can easily find, obtain, and understand security advisories and updates.
- Help customers keep their systems current and up-to-date, to minimize the risk of security issues.
- Work with other vendors of Linux and open source software, including our competitors, to reduce the risk of security issues through information sharing and peer review.

Standards of service

The Red Hat Security Response Team ensures that:

- All email communications sent to the Security Response Team is read and acknowledged with a non-automated response within three working days.
- All email communication that does not relate to a security issue found in Red Hat products and services is replied to with a message pointing to this policy with details on more appropriate places to send the communication.

- If the issue is complicated and requires greater attention from Red Hat technical staff, the team will explain this and tell you when we expect to have a response. If prolonged investigations are necessary, the team keeps you informed of our progress at least every five working days, or alternatively provides you with a mechanism to check the status of its progress at any time.
- The Red Hat Security Response Team works with you to identify other organizations such as other open source vendors that you may wish to contact about the issue.

HOW RED HAT ADDRESSES SECURITY FLAWS

The Red Hat Security Response Team follows an internal process in dealing with security issues. This team investigates and verifies the issue, analyzes which products are affected, determines the impact, and works out the remedial action that needs to be taken.

In cases where a security update needs to be produced, the Red Hat Security Response Team works to ensure that the fix causes minimal side effects. The team will also work with you to determine an appropriate public notification date.

The leader of the Red Hat Security Response Team has stated that the responsiveness of any given open source project to a security issue depends on the project and the seriousness of the issue, and that many of the larger projects, for example, Apache, Mozilla, Linux kernel, have their own security response teams.

For some issues, the finder of the vulnerability will contact the open source projects directly and give them time to produce fixes before disclosing the issue publicly. In other cases, the open source project needs to react to an issue that is already public.

"A good example of reaction time was with a Linux kernel flaw. On Saturday 9 February an exploit was made public that allowed a local unprivileged user to gain root privileges on some Linux kernels (CVE-2008-0600). Within a few hours of it being reported to the kernel mailing list, on 10 February, patches were being exchanged and tested. Later the same day the patches were committed and a new upstream kernel version was released," according to the Red Hat Security Response Team.

With a Linux distribution, security is managed by a single vendor, which can be preferable to having to subscribe to the security lists of all the different open source components being used.

Red Hat monitors a number of sources for details about security issues in any of the thousands of open source projects that make up our distributions, backports patches to correct the issues, and release tests updates. Should an open source project not be responsive to a security issue, the vendors work together to come up with a peer-reviewed patch.

SECURITY MEASUREMENT

The Red Hat Security Response Team is committed to providing tools and data to help security measurement. Part of this commitment is participation at board level in the Mitre CVE and OVAL projects. Red Hat also provides reports and metrics, but more importantly provides the raw data so that customers and researchers can produce their own metrics for their unique situations. This information is available at **www.redhat.com/security/data/metrics/**.

OVAL DEFINITIONS

OVAL definitions are available for all vulnerabilities that affect Red Hat Enterprise Linux 3, 4, and 5:

- OVAL definitions (consolidated xml file, .bz2)[5] (constantly updated)
- OVAL repository (separate files)[6]

VULNERABILITY STATEMENTS

The Red Hat Security Response Team publishes official statements for vulnerabilities currently under investigation and for vulnerabilities that do not affect Red Hat products. These are also available directly from the National Vulnerability Database:

- CVE statements (xml)[7] (updated twice per day)

VULNERABILITY DATA

CVE to date and CVE to severity mapping

This data source is a mapping of the CVE name to the date that the issue was first known to the public. This can help generate statistics based on "days of risk." We also use this data source to capture the severity of issues and how we found out about the issue (date and source). Although the dates may come from third parties, the severity classifications are given by the Red Hat Security Response Team, are specific to Red Hat, and will vary for other distributions and vendors.[8] This file is created manually, and Red Hat updates it every week or two, or by request by contacting **secalert@redhat.com**.

- cve_dates.txt[9] (updated 2009-04-01)

Red Hat Security Advisories to date mapping

This data source is a mapping of Red Hat Security Advisories to the date and time the advisory was issued. Most of this data comes automatically from Red Hat Network, but we've annotated a few entries that needed manual adjustment:

- release_dates.txt[10] (updated twice a day)

Red Hat Security Advisories to CVE and CPE mapping

This data source is a mapping of Red Hat Security Advisories to the vulnerabilities fixed, identified by CVE name. The file contains the product names affected in CPE format (with package name appended) so the file can be filtered by a product or package subset.

- rhsamapcpe.txt[11] (updated twice a day)

CPE list for default installations

Red Hat Enterprise Linux ships with a large number of packages, but they are not all installed by default. These files give lists of packages in default installations that can be used to filter the metrics (format is CPE name with package name appended).

- Red Hat Enterprise Linux 5 (default install)[12]
- Red Hat Enterprise Linux 4 AS (default install)[13]

CPE dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. For reference we provide a dictionary mapping the CPE names we use to Red Hat product descriptions. Some of these CPE names will be for new products that are not in the official CPE dictionary and should therefore be treated as temporary CPE names.

- cpe-dictionary.xml[14] (updated automatically)

Data analysis

This Perl script is designed to run reports based on the data sources cve_dates, release_date, and rhsamapcpe above. For a given product, such as Red Hat Enterprise Linux, and date range it can list all the issues fixed by severity and give a "days of risk" metric as well as vulnerability workflow statistics. For example, run

```
perl daysofrisk.pl —cpe enterprise_linux:5 —severity C
```

- daysofrisk.pl[15] (updated 2009-02-23)

Reports

Based on the above data sets and using daysofrisk.pl you can run sample reports. Here are some pre-generated examples:

DISTRIBUTION	DATES	SEVERITY	METRICS
Red Hat Enterprise Linux 3 (all packages)	20031204-20090401	• all dates • critical flaws	• 133 vulnerabilities[16] • Average is 2.5 days • Median is one day • 83% were within one day
Red Hat Enterprise Linux 4 (all packages)	20050215-20090401	• all dates • for all flaws regardless of severity	• 1302 vulnerabilities[17] • Average is 71.6 days • Median is 15 days • 31% were within one day
Red Hat Enterprise Linux 4 AS (default installation packages)	20050215-20090401	• all dates • critical flaws	• 10 vulnerabilities[18] • Average is 1.9 days • Median is zero days • 90% were within one day
Red Hat Enterprise Linux 5 (default installation packages)	20070314-20090401	• all dates • for all flaws regardless of severity	• 427 vulnerabilities[19] • Average is 60.9 days • Median is two days • 49% were within one day
Red Hat Enterprise Linux 5 (all packages)	20070314-20090401	• all dates • critical flaws	• 73 vulnerabilities[20] • Average is 0.6 days • Median is one day • 98% were within one day

Here is a current report generated on 17 April:

perl daysofrisk.pl –cpe enterprise_linux:5 –severity C
Product: Red Hat Enterprise Linux 5 (all packages)
CPE: cpe:/:redhat:enterprise_linux:5
Severity: Critical
Dates: 20070314 - 20090417 (766 days)
42 advisories (C=35 M=7)
79 vulnerabilities (C=79)
Advisory Workload index is 0.05
Vulnerability Workload index is 0.10
Average is 2 days
Median is 1 days
34% were 0 day
91% were within 1 day
92% were within 7 days
100% were within 14 days
100% were within 31 days
100% were within 90 days

RED HAT ENTERPRISE LINUX 4 SECURITY PERFORMANCE

Red Hat recently released an evaluation of the security status and performance of Red Hat Enterprise Linux 4 from the time it was released to the present. For the full report, see **magazine.redhat.com/2009/03/10/risk-report-four-years-of-red-hat-enterprise-linux-4/**.

We measure the overall risk of running Red Hat Enterprise Linux 4 as a function of two factors: the vulnerabilities and the threats. Our first section covers the security vulnerabilities found in packages that are part of Red Hat Enterprise Linux 4 and the advisories that address them. Our second section covers the threats by examining actual exploitation of those vulnerabilities through exploits and worms.

All the data used to generate this report, tables, and graphs apply to Red Hat Enterprise Linux 4 AS from release day, 15 February 2005, to 14 February 2009, unless otherwise stated.

The aim of this report was to get a measure of the security risk to users of Red Hat Enterprise Linux 4 during the first four years since release. We've shown that although on the surface it looks like Red Hat released a large number of security advisories, many of them do not apply to usual or default installations, and only a very small subset are a high risk. We've shown:

- A default installation of Red Hat Enterprise Linux 4 AS was vulnerable to ten critical security issues over the first four years.
- A customized installation of Red Hat Enterprise Linux 4, selecting every package, would have been vulnerable to 114 critical browser security issues, and 16 in non-browser packages in the four years. Approximately 87 percent of those vulnerabilities had fixes to correct them available from Red Hat Network within one calendar day of them being known to the public.

- Red Hat knew about 51 percent of security issues affecting the first four years of Enterprise Linux 4 in advance. The average time between Red Hat knowing about an issue and it being made public was 21 days (median 9 days).
- We found public exploits for 59 vulnerabilities that could have affected a customized full installation, although the majority relied on user interaction or non-default settings. Attempts to use many of the exploits would be caught by standard Red Hat Enterprise Linux 4 security innovations.
- The most likely successful exploits allowed a local unprivileged user to gain root privileges on an unpatched Enterprise Linux 4 machine.
- Two worms targeting Linux systems were found during the four years, but both affected third-party PHP applications not shipped in Red Hat Enterprise Linux 4. In addition, an update to PHP released over three months before one of the worms was released protected systems that had installed the third party applications.

It would be foolish to draw conclusions about the future state of security in Red Hat Enterprise Linux 4 solely on the basis of this analysis of the past, however what we've tried to do is to enumerate the level of vulnerability and threat and hence overall platform risk. Red Hat treats vulnerabilities in our products and services seriously, and the policies of the Red Hat Security Response Team are specifically designed to reduce the risk from security vulnerabilities:

- We place an emphasis on providing the fastest possible, highest quality turnaround for critical vulnerabilities. We have a Security Response Team distributed global that can draw on significant Engineering and Quality resources to get fixed quickly the things that matter the most.
- We release updates for critical and important security issues as soon as possible rather than batching them into monthly or quarterly updates.
- We provide transparency in the handling of vulnerabilities, our methods, and our metrics.

All of the raw data used to generate the statistics in this report along with some tools to analyze them are available from the Red Hat Security Response Team.[21] We also provide other tools and data that can help security measurement, including CVE mappings for all our advisories and OVAL definitions.

CERTIFICATIONS AND EVALUATIONS

Red Hat Enterprise Linux is certified by all of the industry's software and hardware leaders, providing customers with the value of a broad ecosystem of certified applications and hardware platforms. Red Hat Enterprise Linux has passed the Common Criteria process 12 times on four different hardware platforms. Red Hat Enterprise Linux 5 has even received Common Criteria certification at Enterprise Assurance Level 4 (EAL 4+) under the Controlled Access Protection Profile (CAPP), Label Security Protection Profile (LSPP), and the Role-Based Access Control Protection Profile (RBACPP), providing a level of security and a feature set that was previously unheard of from a mainstream operating system. To learn more, see **www.redhat.com/solutions/government/certifications/**.

United States government agencies are key customers for Red Hat and have been actively involved in ensuring Red Hat meets applicable standards, including:

Security and hardening guides

- National Security Agency (NSA) SNAC Security and Hardening Guide for Red Hat Enterprise Linux 5
  - **www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml**
  - **www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf**
  - **www.nsa.gov/ia/_files/os/redhat/rhel5-pamphlet-i731.pdf**
- Red Hat Enterprise Linux 4 Security Guide
  - **www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/en-US/Security_Guide/**

Directorate of Central Intelligence Directive (DCID) 6/3

Red Hat Enterprise Linux has been used in systems from Protection Level 3 (PL3) up to PL5. For more information, contact your Red Hat account representative.

DISA Security Technical Implementation Guides (STIGs)

Red Hat Enterprise Linux can easily meet the requirements of the DISA STIGs[22]. The Red Hat Government group has implementation tools that can help.

NISPOM Chapter 8

Red Hat Enterprise Linux provides out-of-the-box compliance with the NISPOM Chapter 8 audit requirements. A sample implementation can be found in /usr/doc/audit-1.5.2/nispom.rules in Red Hat Enterprise Linux 4 and 5.

FIPS 140-2

In Red Hat Enterprise Linux 4 and Red Hat Enterprise Linux 5, Red Hat provides FIPS 140-2 certified cryptography through the Network Security Services (NSS) libraries. These libraries are certified to Level 1 and Level 2. The original certification is **csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt815.pdf** and ongoing validation compliance is affirmed by Red Hat in accordance with the FIPS 140-2 Implementation Guidance, G.5[23].

All the NSS code that is subject to FIPS 140 guidelines and that was FIPS validated is in a shared library module called the "Soft Token" (/usr/lib/libsoftokn3.so on Red Hat Enterprise Linux). The Soft Token module that was submitted to NIST and FIPS validated was version 3.11.4. NSS 3.11.4, NSS 3.11.5, and NSS 3.11.7 all include Soft Token 3.11.4.

CONCLUSION

Red Hat Enterprise Linux is developed using open source software principles, offering technology innovation beyond proprietary alternatives. The more people who have access to source code and can employ their expertise to examine it, the fewer secrets are embedded in the code. As a direct result, code becomes more secure. Red Hat Enterprise Linux is reviewed, tested, and certified for enterprise use, and ongoing security is guaranteed by a robust security process and a dedicated security team.

Leveraging the open source development model and its broad ecosystem of certified applications and hardware platforms, Red Hat Enterprise Linux delivers true value to enterprise customers through its fast innovation, established security, and reliable performance.

SOURCES

1 www.linuxfoundation.org/publications/linuxkerneldevelopment.php
2 www.redhat.com
3 http://nvd.nist.gov/
4 http://nvd.nist.gov/download/vendorstatements.xml
5 http://www.redhat.com/security/data/oval/com.redhat.rhsa-all.xml.bz2
6 http://www.redhat.com/security/data/oval/
7 http://www.redhat.com/security/data/metrics/cvestatements.xml
8 http://www.redhat.com/security/updates/classification/
9 https://www.redhat.com/security/data/metrics/cve_dates.txt
10 https://www.redhat.com/security/data/metrics/release_dates.txt
11 https://www.redhat.com/security/data/metrics/rhsamapcpe.txt
12 https://www.redhat.com/security/data/metrics/cpelist-rhel5server-default-install.txt
13 https://www.redhat.com/security/data/metrics/cpelist-rhel4as-default-install.txt
14 https://www.redhat.com/security/data/metrics/cpe-dictionary.xml
15 https://www.redhat.com/security/data/metrics/daysofrisk.pl
16 http://www.redhat.com/security/data/metrics/summary-all-critical.html
17 http://www.redhat.com/security/data/metrics/summary-rhel4-all.html
18 http://www.redhat.com/security/data/metrics/summary-rhel4-critical.html
19 http://www.redhat.com/security/data/metrics/summary-rhel5-all.html
20 http://www.redhat.com/security/data/metrics/summary-rhel5-critical.html
21 https://www.redhat.com/security/data/metrics/
22 http://iase.disa.mil/stigs/index.html
23 http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

LEARN MORE ABOUT RED HAT CONSULTING

www.redhat.com/consulting

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

Turkey: 00800 448 820 640
Israel: 1809 449 548
UAE: 80004449549

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

ASEAN: 800 448 1430
Australia and New Zealand: 1800 733 428
Greater China: 800 810 2100
India: +91 22 3987 8888
Japan: 0120 266 086
Korea: 080 708 0880

NORTH AMERICA
1-888-REDHAT1
www.redhat.com

LATIN AMERICA
+54 11 4341 6200
www.latam.redhat.com
info-latam@redhat.com

www.redhat.com
#1121286_0609