



Achieving PCI Compliance: How Red Hat Can Help

Akash Chandrashekar, RHCE . Red Hat
Daniel Kinon, RHCE . Choice Hotels Intl.

Agenda

- Understanding Compliance
- Security Features within Red Hat
- Backporting
- Choice Hotel's Compliance Challenge
- How Red Hat Satellite can assist in achieving compliance

PCI Compliance basics

- One the most important security concerns in computing is around data breach incidents of cardholder information.
- The incidents are have become more common, prevalent and sophisticated.
- In an effort to thwart such threats, the payment card industry has worked on developing and implementing security standards to help protect cardholder data.
- In December 2004, Visa and MasterCard defined a common set of data security requirements which resulted in the Payment Card Industry Data Security Standard (PCI DSS). These standards were then endorsed by American Express, Discover, JCB and Diners Club.

PCI Compliance Requirements

- PCI identifies 12 requirements which **MUST** be met by any merchant or service provider that stores, processes or transmits credit card information.
- These 12 requirements are further subdivided into over 250 granular audit points which collectively focus on the establishment of strong end-user access controls, activity monitoring and logging, and the need to regularly test security systems and processes.
- These requirements require organizations have strong end- user access controls and activity monitoring and logging need to regularly test security systems and processes.

What??? More Requirements?

- The PCI program also set forth standards for the security of all system that are connected to the overall payment network.

These components include:

- Firewalls, intrusion detection systems, switches, routers, network appliances
- Web servers, applications, databases, DNS, mail servers
- Authentication systems
- POS systems
- Card scanners
- E-commerce web sites

How Red Hat Can Assist With Compliance

Security Response
Team

2009 CVE

CVE-2009-0040

2008 CVE

2007 CVE

2006 CVE

2005 CVE

2004 CVE

2003 CVE

2002 CVE

2001 CVE

2000 CVE

1999 CVE

CVE-2009-0040

Impact: Moderate ([classification](#))**Public:** February 19 2009**Bugzilla:** [486355](#): CVE-2009-0040 libpng arbitrary free() flaw

Details

The MITRE CVE dictionary describes this issue as:

The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.

Find out more about CVE-2009-0040 from the [MITRE CVE dictionary](#) and [NIST NVD](#).

CVSS v2 metrics

Base Score:	6.8	Base Metrics:	AV:N/AC:M/Au:N/C:P/I:P/A:P
Access Vector:	Network	Confidentiality Impact:	Partial
Access Complexity:	Medium	Integrity Impact:	Partial
Authentication:	None	Availability Impact:	Partial

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 (firefox)	RHSA-2009:0315	March 05 2009
Red Hat Enterprise Linux version 5 (firefox)	RHSA-2009:0315	March 05 2009
Red Hat Enterprise Linux version 2.1 (seamonkey)	RHSA-2009:0325	March 05 2009
Red Hat Enterprise Linux version 3 (seamonkey)	RHSA-2009:0325	March 05 2009
Red Hat Enterprise Linux version 4 (seamonkey)	RHSA-2009:0325	March 05 2009
Red Hat Enterprise Linux version 2.1 (libpng)	RHSA-2009:0333	March 04 2009



Vulnerability/Threat Assessment

Impact

Description

Critical	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms.
Important	This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.
Moderate	This rating is given to flaws that may be harder or more unlikely to be exploitable but given the right circumstances could still lead to some compromise of the confidentiality, integrity, or availability of resources.
Low	This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.



RHSA-2005:165 - Security Advisory

[+ create new cloned errata](#)[Details](#) [Packages](#) [Affected Systems](#)

Synopsis

Low: rsh security update

Issued: 2005-06-08

Updated: 2005-06-08

Topic

Updated rsh packages that fix various bugs and a theoretical security issue are now available.

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

Description

The rsh package contains a set of programs that allow users to run commands on remote machines, login to other machines, and copy files between machines, using the rsh, rlogin, and rcp commands. All three of these commands use rhosts-style authentication.

The rcp protocol allows a server to instruct a client to write to arbitrary files outside of the current directory. This could potentially cause a security issue if a user uses rcp to copy files from a malicious server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has

Red Hat Features

PCI Control Objective	PCI Requirement	How Red Hat addresses the requirement.
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and security parameters	IPTABLES & SELINUX Upon Install ability to choose strong passwords, and is also guided with suggestions for strong password choices. No default password is set upon installation. Red Hat also gives the Administrator the option of choosing various strengths for password encryption

Red Hat Features

<p>Protect Card Holder Data</p>	<p>3. Protect Stored Data</p> <p>4. Encrypt transmission of card holder data and sensitive information of across public networks</p>	<p>Red Hat achieves this requirement by offering multiple mechanisms for encryption of stored data such LUKS Encryption, GPG,and SSL.</p> <p>In addition additional steps can be used to secure data by the use of SELINUX contexts.</p> <p>For “Data in motion”, addresses the issue with ability to use VPN, and ssh (tunnels),and SSL encryption.</p>
---------------------------------	--	--

Red Hat Features

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Red Hat addresses the requirement by providing customers with RHN and Satellite for security updates, as well as providing an efficient tool for deployment, and patch management.

In addition Red Hat advisories are provided for all vulnerabilities and available publicly:
Contain a severity impact

Rating contains links to get more information about each issue
•<http://www.redhat.com/security/transparent/cve/>

Red Hat Features

Implement Strong Access Control Measures

7. Restrict access to data by business “need to know”

8. Assign a unique ID to each person with computer access

9. Restrict access to card holder data

Red Hat addresses the three requirements with use of Red Hat Directory Server. By employing a mechanism of role-based authentication - users are granted access, only as needed.

Red Hat also offers Meta-Matrix which offers ability for granular control of data views, and access definition of those views.

Red Hat Features

Regularly monitor and test networks

10. Track and monitor all access to network and card holder data

11. Regularly Test security systems and processes

rsyslog

SELINUX, “Se-Troubleshoot” is an excellent tool to be able to capture attempts to intrude a system.

With the advent of RHN, and Satellite, systems receive information about threats and vulnerabilities (CVES), as well as severity of the threat and or vulnerability.

http://www.redhat.com/security/updates/backporting/?sc_cid=3093

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

Red Hat Features

Maintain an Information Security Policy	12. Maintain a policy that addresses information security	(DES, MD5,SHA) , SSL SSH for encrypted transmission SE-LINUX Capability to enforce password expiration (chage,quota) Userbased/Rolebased authentication LDAP, Directory Server
---	---	---

Daniel Kinon

Sr. Linux Systems Administrator

Choice Hotels International

RHCE #805009758339922

If I could be a cereal box character, I would be Snap because I'm first, I'm witty and crackle and pop just sound like accidents waiting to happen.



The Choice Hotels Compliance Challenge

- The Puzzle
- The Pieces
- The Tools
- The Solution

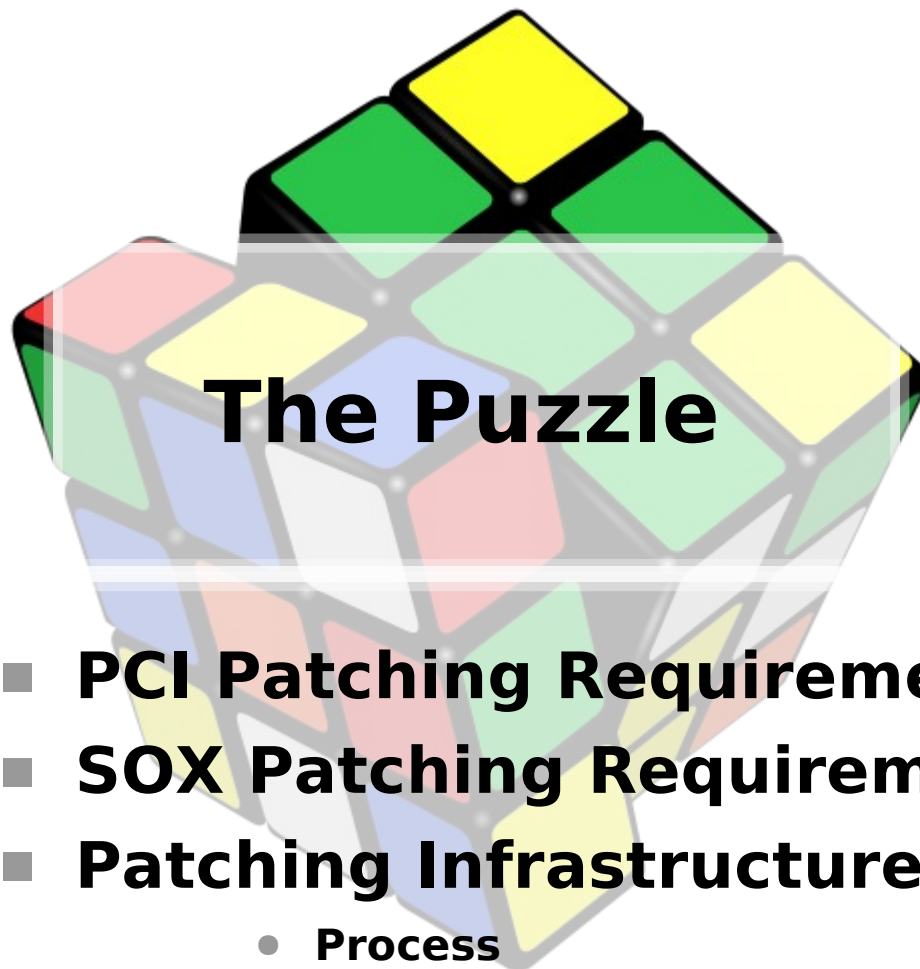
WHAT WOULD
YOU ATTEMPT
TO DO IF YOU
KNEW YOU
COULD NOT FAIL?
(LINKEDIN)

“ I need a way to deploy & patch my systems and handle PCI compliance. Our PCI patching criteria requires us to update packages with applicable security errata within in 30 days of the errata's published date.”

- Daniel Kinon, RHCE . Choice Hotels Intl.

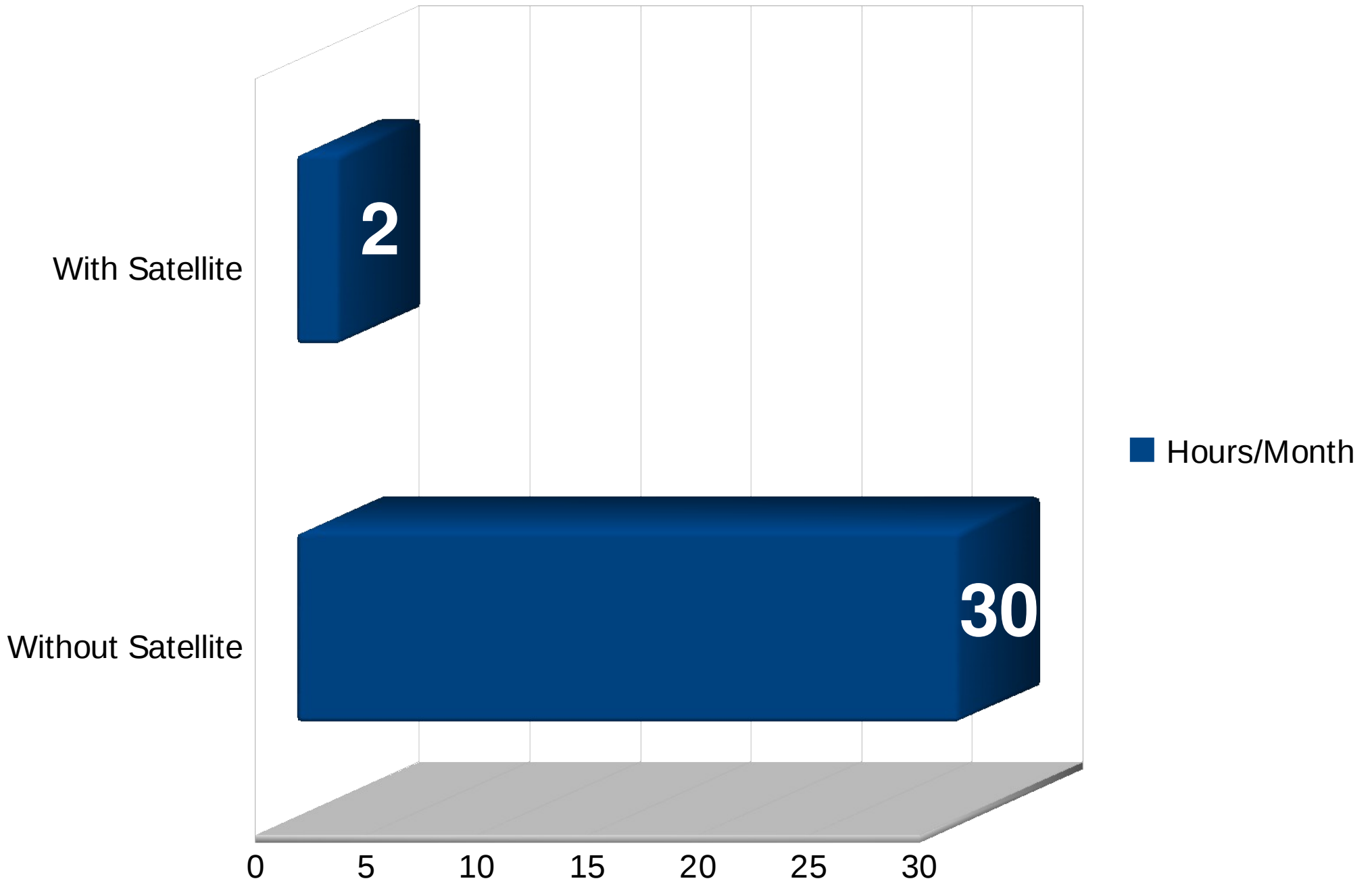


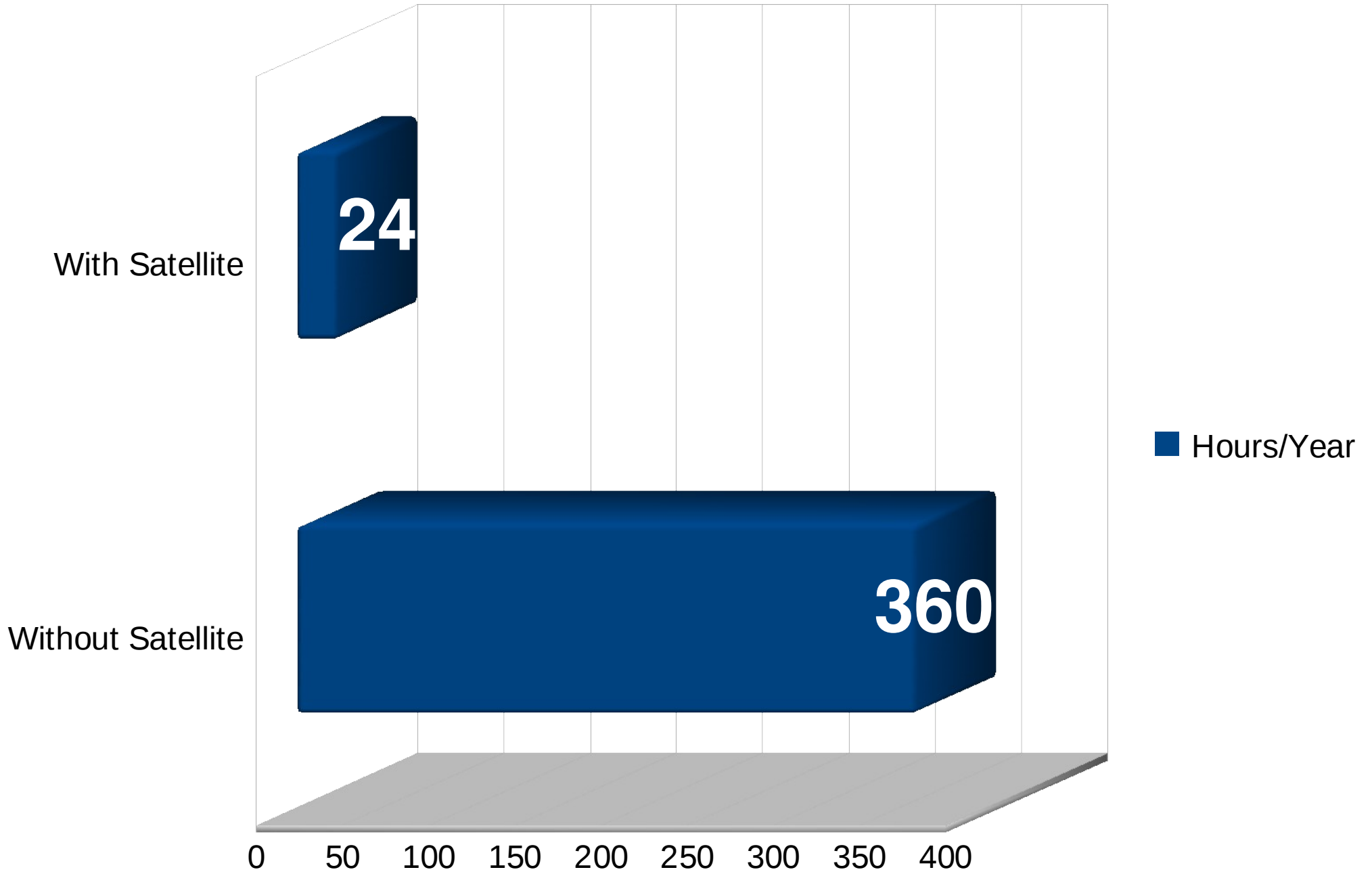
System Repair Tool

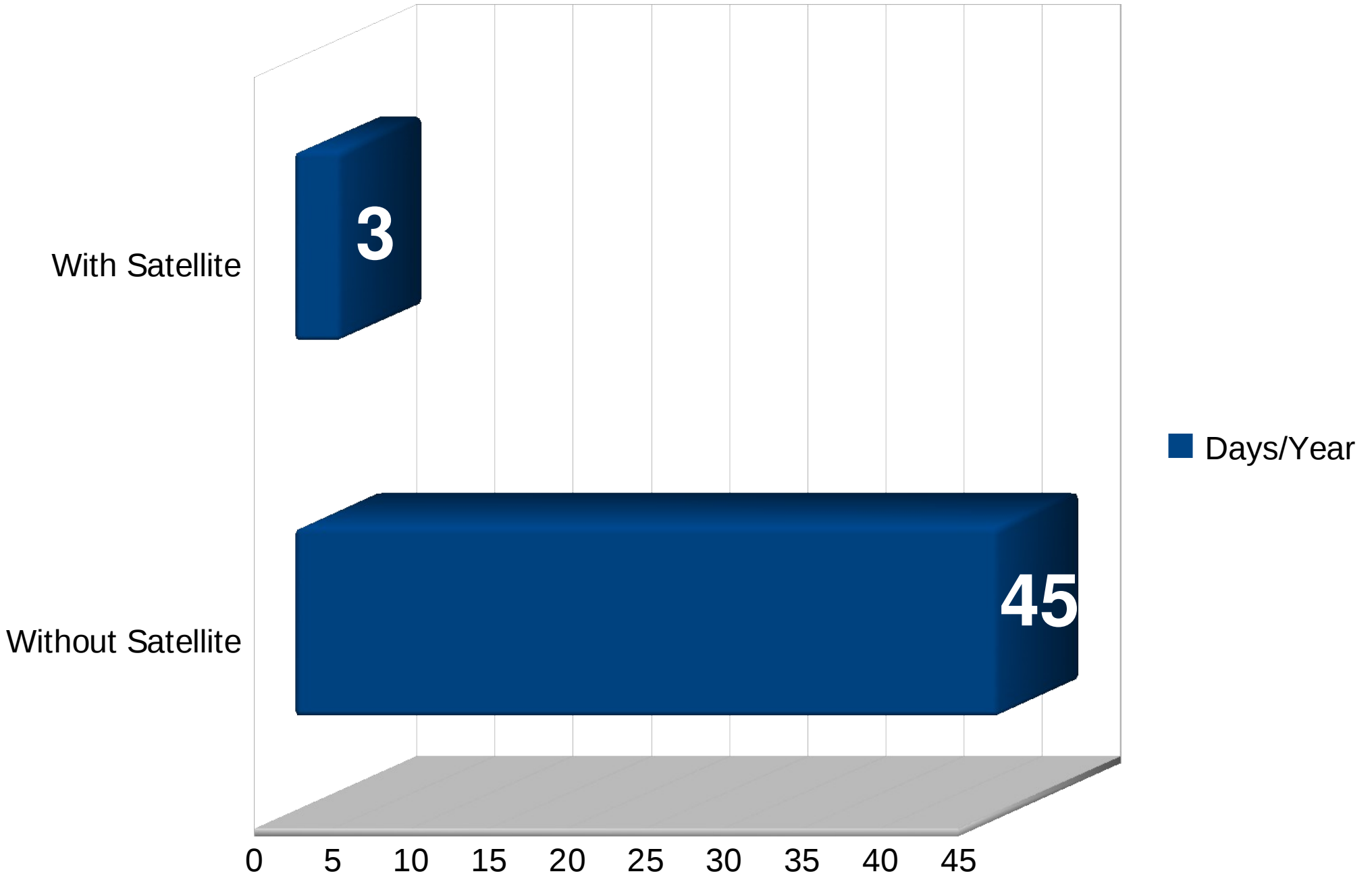


The Puzzle

- **PCI Patching Requirements**
- **SOX Patching Requirements**
- **Patching Infrastructure**
 - **Process**
 - **Organization**
 - **Delegation**
- **Audit Reporting**







Poor Planning?

Help Me !!!!



[Your RHN](#)[Systems](#)[Errata](#)[Channels](#)

*"Satellite will help us manage our systems in several ways. It will allow us to group systems, making patching easier. It will allow us to assign people access to those groups allowing us to delegate patching like never before. Overall Satellite will help us by greatly reducing the work load associated with our patching process."
- Daniel Kinon, RHCE . Choice Hotels Intl.*

[Overview](#)[Systems](#)[System Groups](#)[System Set Manager](#)[System Entitlements](#)[Advanced Search](#)[Activation Keys](#)[Stored Profiles](#)[Custom System Info](#)[Kickstart](#)

Create System Group

Create a system group using the form provided. Note that the group will be empty until systems with an asterisk (*) are **required**.

* - Required Field

Name*


Description*

BUY NOW!

Add systems
Renew service
Manage & provision

[Your RHN](#)[Systems](#)[Errata](#)[Channels](#)[Schedule](#)[Users](#)[Help](#)

Systems

 Search

1 SY

[Overview](#)[Systems](#)[System Groups](#)[System Set Manager](#)[System Entitlements](#)[Advanced Search](#)[Activation Keys](#)[Stored Profiles](#)[Custom System Info](#)[Kickstart](#)**BUY NOW !**

Add systems

Renew service

Manage & provision



Create Activation Key

Description:**Key:****Usage Limit:** (Leave blank for unlimited use)**Base Channel:****Entitlement:****Universal default:**



The Pieces

- **List of Servers w/ Applicable Errata**
- **Errata Type (RHSA vs. RHBA)**
- **Errata Published Date**
- **Server Patching Process**
- **Patch Application Date**
- **Final Compliance Report**



Vulnerability/Threat Assessment

Impact

Description

Critical

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms.

Important

This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.

Moderate

This rating is given to flaws that may be harder or more unlikely to be exploitable but given the right circumstances could still lead to some compromise of the confidentiality, integrity, or availability of resources.

Low

This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.



RHSA-2005:165 - Security Advisory

[+ create new cloned errata](#)[Details](#) [Packages](#) [Affected Systems](#)

Synopsis

Low: rsh security update

Issued: 2005-06-08

Updated: 2005-06-08

Topic

Updated rsh packages that fix various bugs and a theoretical security issue are now available.

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

Description

The rsh package contains a set of programs that allow users to run commands on remote machines, login to other machines, and copy files between machines, using the rsh, rlogin, and rcp commands. All three of these commands use rhosts-style authentication.

The rcp protocol allows a server to instruct a client to write to arbitrary files outside of the current directory. This could potentially cause a security issue if a user uses rcp to copy files from a malicious server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has



The Tools

- **Red Hat Satellite**
 - Package Management
 - Satellite API
- **API Supported Scripting Language**
 - Perl
 - Java
 - Python
- **Other APIs (*Optional*)**

API Example

```
#!/usr/bin/perl -w

use Frontier::Client;
Use strict;

# Login and create session
my $client = new Frontier::Client(url => "http://<satellite server hostname>/rpc/api");
my $session = $client->call('auth.login', <username>, <password>);

# List Software Channels: returns an array (arrayref) of structs (hashrefs)
my $channels = $client->call('channel.listSoftwareChannels', $session);

# List Systems: returns an array (arrayref) of structs (hashrefs)
my $systems = $client->call('system.listUserSystems', $session);
Foreach my $system (@$systems) {
    My $id = $system->{id};
    # Get Event History per System: returns an array (arrayref) of structs (hashrefs)
    my $sysEvents = $client->call('system.getEventHistory', $session, $id);
}

# Logout
$client->call('auth.logout', $session);
```

References

- <https://rhn.redhat.com/rhn/apidoc/index.jsp>
- <https://fedorahosted.org/spacewalk/wiki/SpacewalkApiPerlGuide>

The Solution

“Our PCI patching criteria requires us to update packages with applicable security errata within in 30 days of the errata's published date. The API solves this in two ways. First, it allows us to see the packages that have been updated and when the updates occurred giving us a reliable patching time line that can be followed. Second, we can compare packages against their corresponding dates and verify (in a report) that the package was patched within the required window. This is great!”

- Daniel Kinon, RHCE . Choice Hotels Intl.

Satellite Reporting

server.example.com

System Information

- **RHN ID:** 1000010028
- **Reg Date:** 2009-06-24 T00:59:45
- **Last Check-in:** 2009-08-28 T22:18:28
- **Vendor:** Dell Computer Corporation
- **System:** PowerEdge 1850
- **Asset Tag:** 3VCRJ91
- **Bios Version:** A04

System Events

<p>Package Install 2009-07-06 23:41:33.0</p> <p>Result: Failed: Some of the packages specified were on a skip list</p> <ul style="list-style-type: none"> ◦ kernel-2.6.9-89.EL ◦ kernel-smp-2.6.9-89.EL ◦ kernel-utils-2.4-18.el4:1
<p>Package Removal 2009-06-30 13:27:12.0</p> <p>Result: [['cscope', '15.5', '10.RHEL4.3', '', 'i386']] removed successfully</p> <ul style="list-style-type: none"> ◦ cscope-15.5-10.RHEL4.3
<p>Package Removal 2009-07-07 04:08:12.0</p> <p>Result: cairo-1.2.4-5.el5 failed because of package not installed cdparanoia-libs-alpha9.8-27.2 failed because of package not installed boost-devel-1.32.0-7.rhel4 failed because of package not installed boost-1.32.0-7.rhel4 failed because of package not installed</p> <ul style="list-style-type: none"> ◦ boost-1.32.0-7.rhel4 ◦ boost-devel-1.32.0-7.rhel4 ◦ cadaver-0.22.1-3 ◦ cairo-1.2.4-5.el5 ◦ Canna-3.7p3-9.el4 ◦ Canna-libs-3.7p3-9.el4 ◦ cdparanoia-alpha9.8-24 ◦ cdparanoia-libs-alpha9.8-24 ◦ cdparanoia-libs-alpha9.8-27.2
<p>Package Install 2009-07-06 23:40:13.0</p> <p>Result: Packages were installed successfully</p> <ul style="list-style-type: none"> ◦ audit-1.0.16-4.el4 ◦ audit-libs-1.0.16-4.el4 ◦ file-4.10-8.el4 ◦ kernel-2.6.9-89.EL ◦ kernel-smp-2.6.9-89.EL ◦ kernel-utils-2.4-18.el4:1 ◦ krb5-libs-1.3.4-62.el4 ◦ mkinitrd-4.2.1.13-4

