

**RED HAT  
SUMMIT**

**LEARN. NETWORK.  
EXPERIENCE OPEN SOURCE.**

June 11-14, 2013  
Boston, MA

RED HAT  
**SUMMIT**

# Managing Updates on Red Hat Enterprise Linux

Scott McBrien  
Curriculum Manager, Red Hat  
June 13, 2013

# Your boxes are out of date!!!!!!!

Maybe not

- Many “Security Scanning” tools report incorrect data
- Perhaps your organization has selected to not apply all updates, but instead certain types of updates



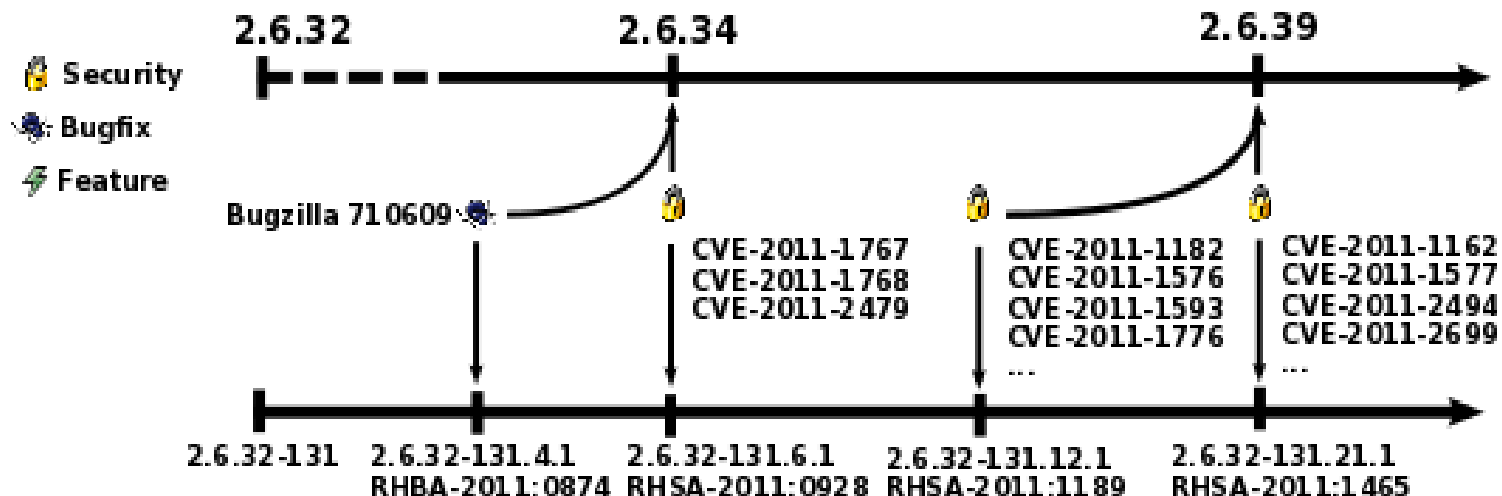
```
[snarky@flyinghotdog ~]$ telnet flyinghotdog 80
Apache/2.2.15 (Red Hat) Server at flyinghotdog Port 80

[snarky@flyinghotdog ~]$ rpm -q httpd
httpd-2.2.15-15.el6_2.1.x86_64
```

# Red Hat Package Maintenance (Backporting)

We backport security fixes, bug fixes, and selected features into Red Hat Enterprise Linux packages

## Open Source kernel



## Red Hat Enterprise Linux kernel

# Using yum updateinfo

Displays a report of outstanding errata

```
[root@desktop1 ~]# yum updateinfo
Updates Information Summary: available
 33 Security notice(s)
     4 Critical Security notice(s)
    10 Important Security notice(s)
    19 Moderate Security notice(s)
 27 Bugfix notice(s)
   3 Enhancement notice(s)
updateinfo summary done
```

Can optionally display Errata with **list**

Note: Severity types

# Exercise! Applying Critical Security Errata

Log in as `root` on your server ( password = `redhat` )

- View a report of outstanding Errata for the machine (save a copy for later)
- Use `yum` to apply all relevant Critical Security updates to your system
- Verify that there are no longer Critical Security updates for your system
- View a report of outstanding Errata for the machine, compare against the previously captured copy. Are there any discrepancies you were not expecting?

# Exercise! Applying Critical Security Errata

Log in as `root` on your server ( password = `redhat` )

- View a report of outstanding Errata for the machine (save a copy for later)
- Use `yum` to apply all relevant Critical Security updates to your system
- Verify that there are no longer Critical Security updates for your system
- View a report of outstanding Errata for the machine, compare against the previously captured copy. Are there any discrepancies you were not expecting?

# RHN Satellite API, An Alternative Errata Management Solution

## Method: **scheduleApplyErrata**

Description: Schedules an action to apply errata updates to multiple systems.

Parameters\*:

string **sessionKey**

array:

int - **serverId**

array:

int - **errataId**

\* There are multiple parameter variants of this API call...

Check out George Hacker's Taste of Training Session:

"Begin Programming Your Red Hat Satellite Server", Friday 11:00a, Room 206



# Ruh-Oh! What Did We Just Do To “Production”?



What could possibly go wrong?!?

Updates should be verified before being applied to “Production” systems

# Designing a Test Environment

The test environment should be as close to “Production” as possible to get the best validity testing

- Same hardware?
- Same software?
  - Development boxes are often used for this purpose, but are typically not the same as “Production” in terms of configuration and additional software

# Designing a Test Environment

The test environment should be as close to “Production” as possible to get the best validity testing

- Same hardware?
- Same software?
  - Development boxes are often used for this purpose, but are typically not the same as “Production” in terms of configuration and additional software

# Validate RPM Content As Well

Can you see what's wrong?

```
[root@desktop1 tmp]# rpm -qpl FluffyMcAwesome-1.0-1.el6.x86_64.rpm  
/tmp/FluffyMcAwesome-1.0.tar.gz
```

```
[root@desktop1 tmp]# rpm -qp --scripts FluffyMcAwesome-1.0-1.el6.x86_64.rpm  
postinstall scriptlet (using /bin/sh):  
cd /tmp  
tar -xf FluffyMcAwesome*  
cd FluffyMcAwesome-1.0  
make  
make install
```

# RPM Scripts and Triggers

Know what your RPMs are doing (as **root**)

- Inspect their scripts using the **--scripts** query
- Inspect any triggers with **--triggers** query

```
rm -f /lib/modules/$(uname -r)/kernel/drivers/scsi/lpfc/lpfc.ko
```

(taken from a vendor's actual %postun script)

You can also inspect the file payload

# Exercise! Choose Wisely...

Log in as `root` on your server ( password = `redhat` )

- Inspect the two **FluffyMcAwesome** RPMs in `/tmp`.
- Based off of your inspection, choose the one that is the best, and install it on your system.
- Why did you choose that one over the other?
- Were there any unintended consequences?

# Additional Questions?

Don't forget your surveys!

# Thank you for attending!!!!

Presentation, and materials available on my people page:

<http://people.redhat.com/~smcbrien>