The Year in Review (in Cray Security)

Wendy Palm, Cray Inc.

- **Changes since last year**
  - Bye bye SLES9
- **By the numbers**
  - SLES9
  - SLES10
  - SLES11
- **Scrambles**
- **Future Plans**

Changes since CUG2011

- **SLES9 no longer supported**

  No more security updates for
  - SMW 1.5/3.1 & Unicos/lc 1.5/2.0
  - XD1

- **ES systems added to security update FNs**
  - Non-Bright-Cluster-Managed
  - BCM

- **SLES11SP2 released**
  - So far, all have installed cleanly on SLES11SP1 systems

Changes since CUG2011

- **Regular cumulative updates** (based on CUG2011 request)
  - Current releases: cumulative FN for every release
  - Older releases: cumulative FN every 6 mos
  - End-of-maintenance: final cumulative FN

- **FN reporting mechanism**
  - Every security FN install script runs SPS's "record.fn"

- **Novell changed style of announcements**

  Same information, slightly different format

  https://hermes.opensuse.org/feeds/63186?page=1

CVE?

CVE - Common Vulnerabilities and Exposures - http://cve.mitre.org/

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

By the Numbers – SLES9

SLES9 – released 8 Mar 2004, maint ended 31 Aug 2011

Most common packages getting updates (in order of frequency):
java, kernel, clamav, ethereal, mozilla, cups, mysql, libpng, freetype2, ruby, XFree86, libexif, mailman, horde, quagga, tomcat, apache, openssh, gd, python, yast2-packagemanager-devel, km_nss, openssl, samba, tk, pcre.

SMW 1.5/3.1 & Unicos/lc 1.5/2.0

- 948 rpms in distribution
- 54 FNs, 965 updates of 255 rpms, 511 CVEs

XD1

- 1420 rpms in distribution (pretty much all of them)
- 29 FNs, 1544 updates of 292 rpms, 670 CVEs

By the Numbers – SLES10

SLES10 – released 17 Jul 2006, maint ends 31 Jul 2013

SMW 3.1.10/4.0 & CLE 2.1/2.2

- 1084 rpms in SMW distribution
- 1299 rpms in CLE 2.1 distribution
- 1025 rpms in CLE 2.2 distribution (rpmreduction project)

39 FNs, 1432 updates of 351 rpms, 1026 CVEs (as of 18Apr)

- Plus 2 cumulative update FNs

By the Numbers – SLES11

SLES11 – released 24 Mar 2009, maint ends 31 Mar 2016

SMW 5.0/5.1 & CLE 3.0/3.1 (SLES11)

- Novell re-organized their rpms – many broke into multiple rpms and many "-devel" rpms were moved into SDK and SLED
- 1075 rpms in SMW distribution
- 1267 rpms in CLE distribution

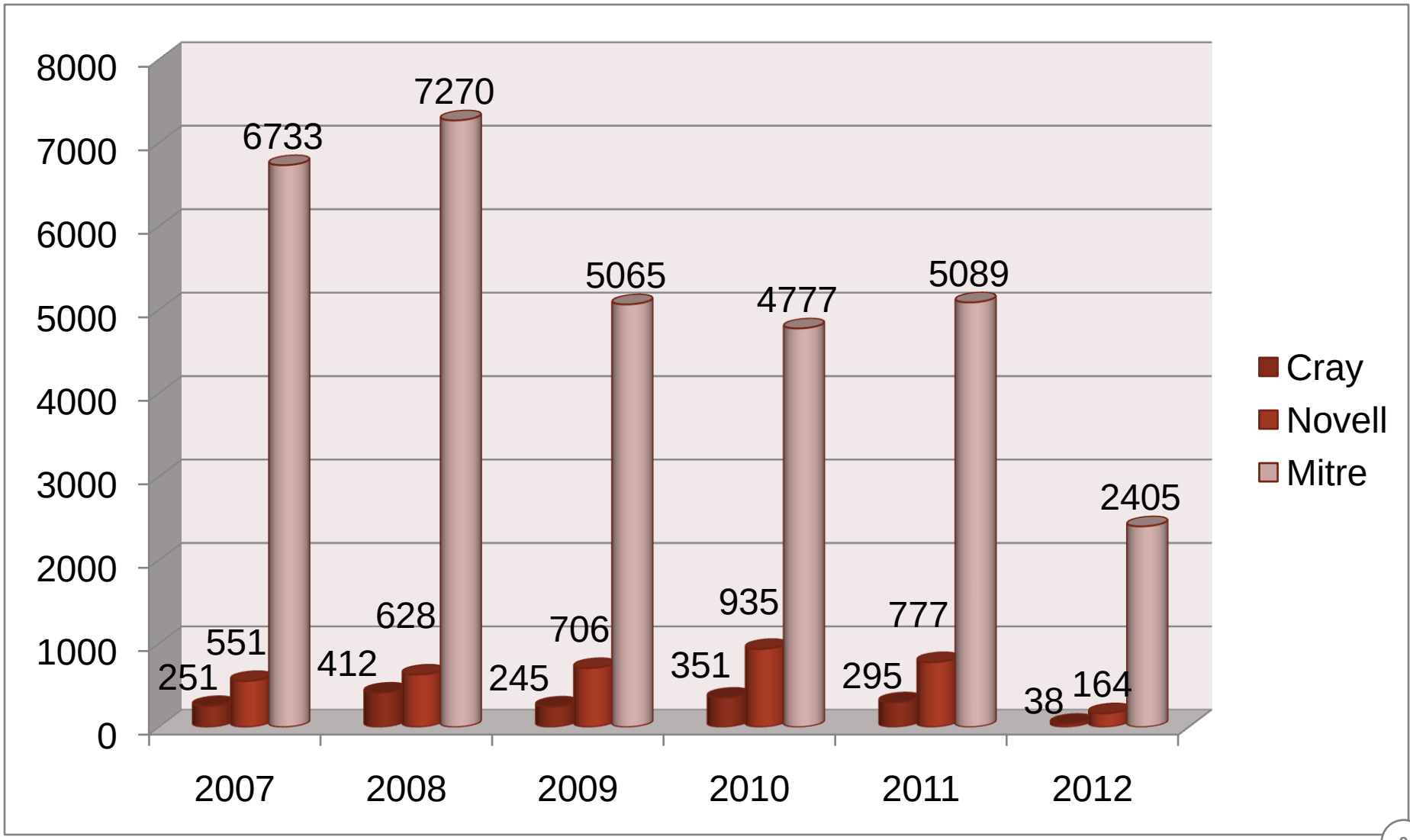
SMW 6.0 & CLE 4.0 (SLES11sp1)

- Many more rpms broke into multiple rpms & we discovered some had gone missing in the initial SLES11 dist.
- 1044 rpms in SMW distribution
- 1292 rpms in CLE distribution

24 FNs, 824 updates of 352 rpms, 558 CVEs (as of 18 Apr)

- Plus, 5 cumulative update FNs (2 SLES11, 3 SLES11sp1)

By the Numbers – CVEs by year



By the Numbers – Scrambles per year

- 2007 – 2 FNs
- 2008 – 3 FNs
- 2009 – 7 FNs
- 2010 – 19 FNs, 5 issues with FNs by architecture & OS
- 2011 – 2 FNs (xorg, pcmd); critical researching 4 times
- 2012 – 1 FN (dropbear); critical researching 2 times

2011 scrambles

- **pcmd (FN5820)**
  - Reported by developer on 29 Aug 2011
  - security hole in Cray code “pcmd”; privilege escalation
  - workaround to remove suid
  - Fix available 11 Oct; fixed in CLE 4.0.UP02

- **xorg (FN5823)**
  - Reported by customer on 03 Nov 2011
  - Security hole in xorg-x11-server; privilege escalation
  - Novell claimed no SLES was affected – we proved them wrong. They argued about it for 10 days before they believed me.
  - Workaround to disable the xorg-server – affected vnc
  - Novell provided updated rpms 23 Nov, FN published with getfix.
  - Fixed in CLE 4.0.UP03
  - Novell now responds to my "please retest your systems; you're wrong" faster.

2012 scrambles

- **Dropbear SSH (FN5852)**
  - Reported by Novell (regular security announcement) 27 Feb 2012
  - Remote user execute arbitrary code
  - Investigation revealed that our use of dropbear makes this vulnerability innocuous. There are no actual user accounts in the initramfs image, and dropbear is not used on service nodes.
  - However, the dropbear version in CLE was updated on 29 Feb for next CLE release.

Scrambles - kernels

Remember, we use the online configuration database maintained by Cray field personnel to determine what sites are running and plan our builds of any potential kernel scrambles.

So, if your entry is out of date, your build may be delayed.

Future Plans

- Expansion of the “record.fn” script with incorporation into SMWinstall and CLEinstall.
- Improved ES instructions (both BCM & nonBCM).
- Better attention given to 3rdParty software – MySQL, etc.
- Any other ideas that would make your security updates better/faster/cleaner?

Reporting security issues

Email to os_security@cray.com

- Provide as much detail as possible, including potential exploit and we'll create an appropriate bug.

Open a bug

- Initial report should have as few details as possible just an overview of the issue; so this can be made "**public**".
- Follow up notes should be "**private**" and contain as much information as possible.
- Assign to "**security**" or at least set "**security**" keyword so I see it quickly.

Go through site personnel

Haben Sie Fragan?

Dankeschön!

Wendy Palm
wendy@cray.com
os_security@cray.com