Scaling Security in a Complex World

Wendy Palm

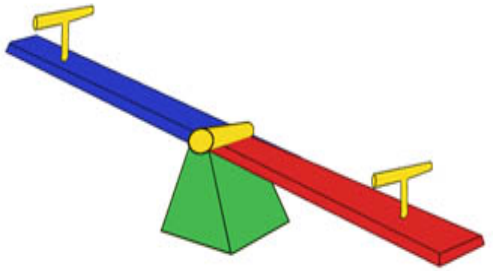
Agenda

- **Purpose**
  - Cray systems are more accessible to “the outside world” than ever before, causing our approach to become correspondingly more concerned with security.
  - Cray now offers a variety of products, and the new security update process simplifies and standardizes this across products.
- **Benefit/Value**
  - New install processes for new products allows site more flexibility.
- **Cray OS security process**
  - Vulnerability classification
  - Timelines
  - Future Plans
- **Summary**
- **Q&A**

Balancing Act

- Security vs usability
- Taking downtime to update vs system availability

- Cray's answer has been to release tested groups of security updates in a regular cadence, with the ability to expedite critical issues.

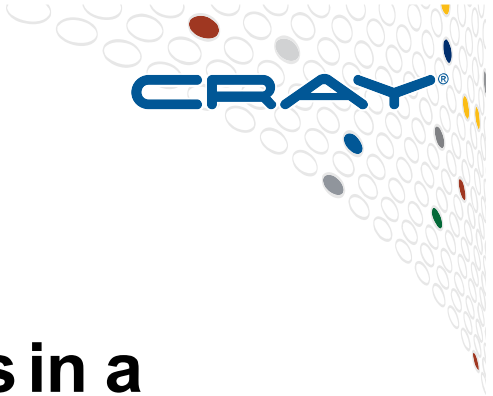


Status Quo isn't enough

- **Cray has more products than ever before.**
- **Sites have multiple Cray products.**
  - And desire similar install/update procedures.
- **Cray customer base is becoming more diverse.**
  - And therefore the systems are used in many different ways, need different packages installed, severity classifications differ.
- **Sites have become more concerned with security.**

The "same old way" just won't cut it anymore.

Security Goal



Provide security updates for all Cray products in a standardized process, on a planned schedule, allowing for priority issues to be handled in an expedited manner.

Cray Changes

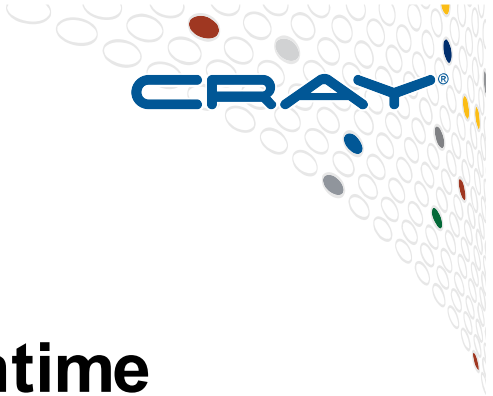
- **Previously, Cray had a single non-dedicated OS security engineer who did all the monitoring, downloading and testing for security updates and when needed, pulled in various developers.**

- **This works for a couple of products, but does not scale well to new products and multiple OSs.**

Cray Changes

- **Cray OS Security team**
  - **No more "single person team" for security**
- **"Early Access" now a standardized process**
  - Previously this was an unpublicized, ad-hoc, unofficial process.
- **More Cray products will be providing security updates.**

Cray Changes



New features targeted to reduce system downtime

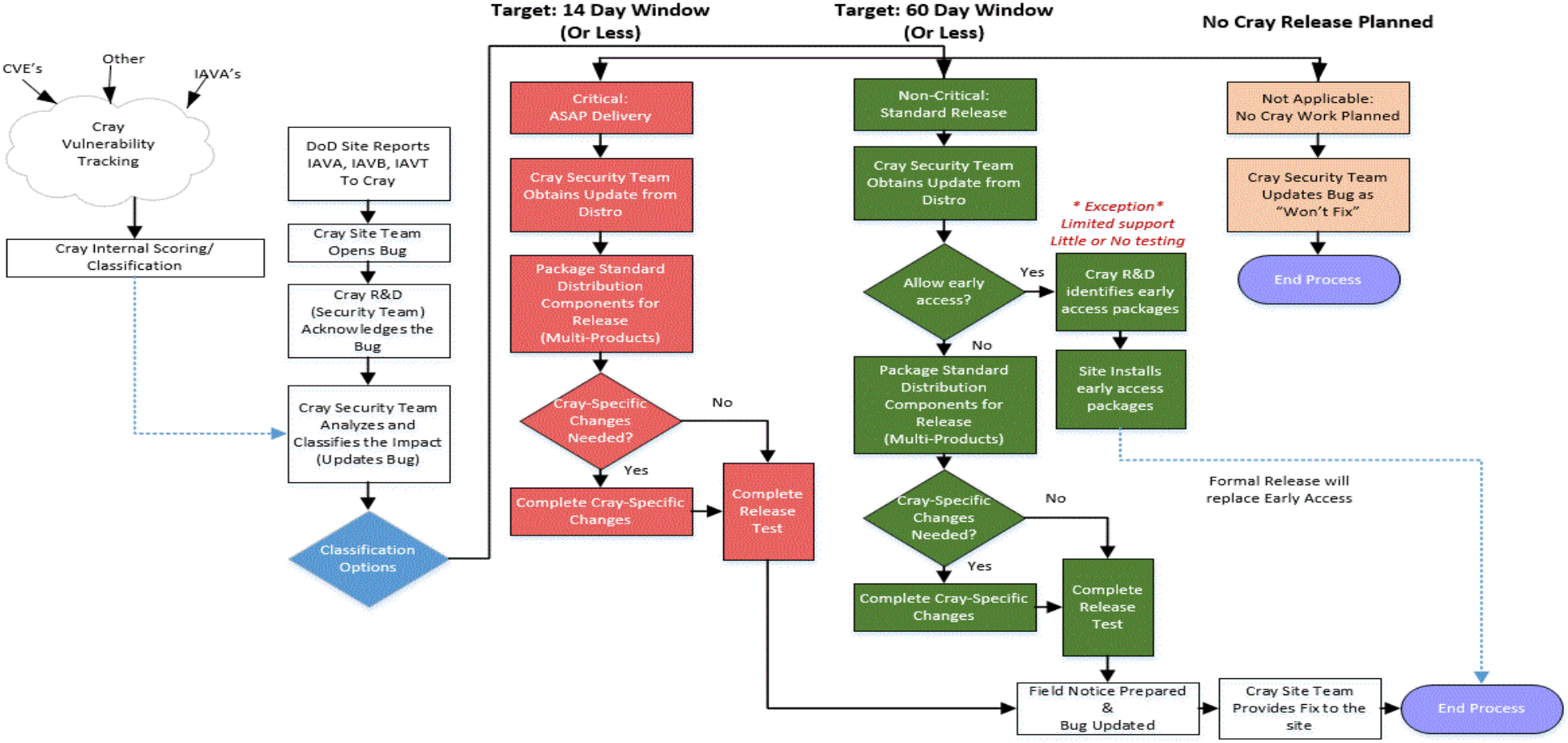
- **Live updates**
- **Rolling reboots**

Cray OS Security Process

Basic process is the same. Cray Security Team will:

- **Receive notification of vulnerabilities**
- **Classify the severity of the vulnerabilities**
- **Get the update(s)**
  - Download binary rpm(s)
  - Get the patch to the developer for Cray-built rpms
- **Test install the update(s) on internal Cray systems**
- **Release the update(s) to sites via Field Notice/Patch**
- **Update(s) are added to future releases**

Cray OS Security Patch Release Process



How is Cray notified of Vulnerabilities?

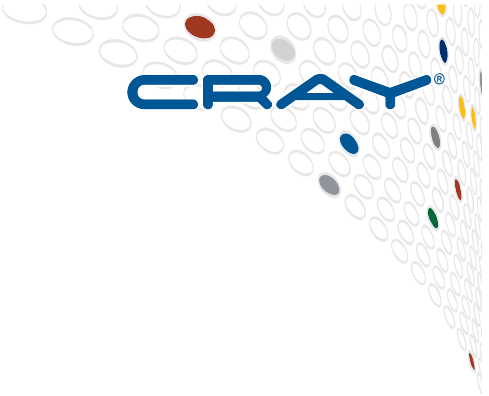
- **Updates from Vendors (Cray actively monitors)**
  - SUSE
  - CentOS

- **Notification from Site**
  - Open a Bug/case, assign to “security”, generic initial description, “public”.
  - Additional commentary and attachments should be as detailed as possible, set to “private”.
  - All communications will be conducted through the bug itself.

Classifying Vulnerabilities

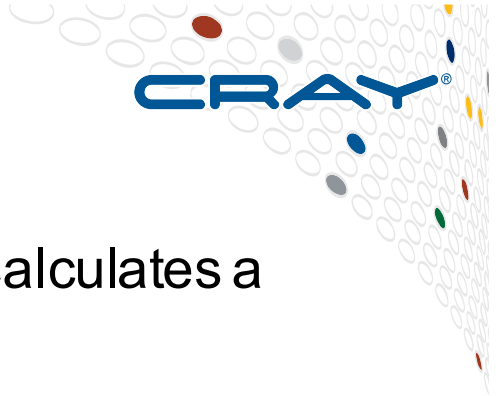
- **Cray Security Team will classify vulnerabilities**
  - High priority task
  - Goal is to have the classification done within 1 business day
    - based upon full availability of required information
- **Three categories**
  - Critical – Provide Fix ASAP
  - Non-Critical – Provide fix in next regularly scheduled Field Notice
  - Not Applicable – No Plan to provide a fix
- **Classifications will be documented in the bug**
  - Site team can work with the Cray Security Team on mismatched expectations on classifications.

CVE



- Common Vulnerabilities and Exposures
- http://cve.mitre.org/
- Dictionary of publicly known information of security vulnerabilities
- Provides a common identifier to enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services

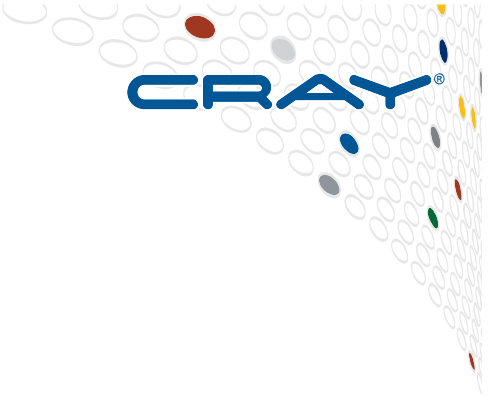
Classifying Vulnerabilities



The CVSS score (Common Vulnerability Scoring System) calculates a numerical value to a vulnerability based on:

- **Access Vector**
- **Access Complexity**
- **Authentication**
- **Confidentiality Impact**
- **Integrity Impact**
- **Availability Impact**
- **Exploitability**

Classifying Vulnerabilities



- **Attack Vector**
  - **Network/Remote**– from outside (website, ssh, telnet, etc.)
  - **Adjacent** – from outside the system, but within the local network
  - **Local** – on the system (current user)
  - **Physical** – need physical access to console/system
- **Attack Complexity**
  - How difficult is it to exploit the vulnerability (**Low/Medium/High**)

Classifying Vulnerabilities

- **Authentication**
  - Does the attacker need to authenticate, and if so, how many times
- **Impact**
  - **Confidentiality** (none/partial/complete)
  - **Integrity** (none/partial/complete)
  - **Availability** (none/partial/complete)
- **Exploitability**
  - Unproven
  - Proof-of-Concept
  - Functional
  - High/Easy

Classifying Vulnerabilities

- **Check CVE database –** see if it's listed, check links
- **Check code patch –** give to developer to evaluate
- **Check other security sites –** several offer good evaluations, some not-so-helpful

- If there is a published exploit with privilege escalation or denial of service, vulnerability severity is set to "critical", a "security scramble" is called and the timeline is accelerated.

Security Update Types

- **Pass-through binary rpms**
  - Rpms that we download directly from the vendor
  - No action by Cray other than the download and install
  - “userland”

- **Cray-built rpms**
  - Requires some action by Cray
  - Build the rpm (CLE kernel)
  - Build dependencies of the rpm (lustre for elogin must match the elogin kernel version)

Security Update Patches – Non-Critical

- **Non-Critical – Timeline Target: 60 Days or Less**
  - **May contain non-kernel and/or kernel updates**
    - May contain Cray-Specific Kernel Modifications
  - **Standard Distribution Updates are Candidates for Early Access Release**
    - Early Access updates will be replaced by the formal Non-Critical Update Release

Early Access

- **Pass-through binary rpms from Vendor**
- **Very little, if any, Cray internal testing**
- **Unsupported by Cray (until official release)**

- **Site may gather rpms from their own local mechanism or request them from Cray**
- **Cray will assist site with installation issues if necessary**
  - If an install is having problems, don't force it – report the problem in a bug

- **This option is provided to assist those sites that have a requirement for a more frequent cadence and are willing to take the risk.**

Security Update Patches - Critical

- **Critical – Timeline Target: 14 Days or less**
  - Same process as non-Critical, but expedited timeline
  - Can contain non-kernel and/or kernel updates
    - May contain Cray-Specific Kernel Modifications
  - No Early Access Release

Security Update Patches - Critical

FN6029, the last kernel critical patch released Jan 2015

- **SMW kernel update – pass through SUSE kernel**
- **Elogin & ESM – pass-through kernel, dependencies**
  - 10 ESL, 2 ESM releases needed getfixes
- **CLE – Cray-built kernel**
  - 15 CLE releases needed getfixes
  - 4.0UP01/2/3, 4.1UP01, 4.2UP00/1/2, 5.0UP01/2/3, 5.1UP00/1/2

Timelines

If a site has delivery commitments that cannot be met by the Cray timelines, you can email os_security@cray.com to ask about the process, but for specific vulnerabilities, requests for early access, please create a bug with those specific requirements. All vulnerability specific communication will be done through the bug.

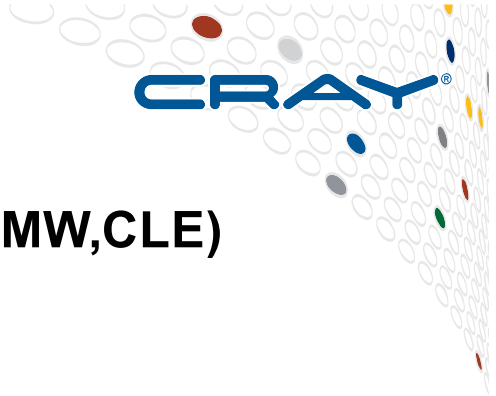
Installing Updates - SLES11

- **Older releases follow the same process as before**
  - Security updates provided in a getfix package with install script
  - Install the rpms via the install script on the SMW
  - Install the rpms via the install script in bootnode root & shared-root
  - Install the rpms via the install script or BCM on the esms & esl
  - Reboot the systems

Installing Updates

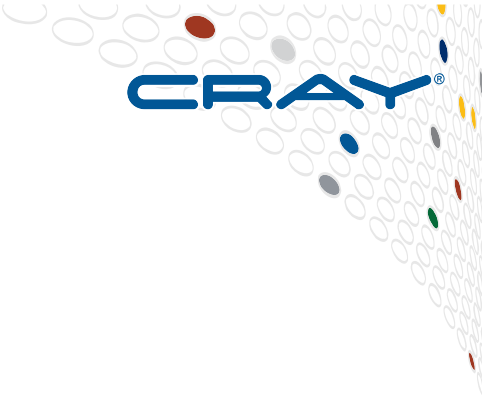
- **All new Cray products follow the same basic process**
  - Security updates provided in an iso, via a patch
  - Load the new rpms into a repository
  - Install the rpms into a image (or the live system)
  - Test update on sample node
  - Boot updates to the whole system

Installation example (SMW 8.0/CLE 6.0)



- **Get SLE patch set (standard patch format, just like SMW,CLE)**
- **The patch set includes:**
  - **SLE_12.SP0.PSX.readme**
    - Patch information
  - **INSTALL**
    - File listing the load, install & deployment steps
  - **SLE_12.SP0.PSX.iso**
    - Rpms that are being updated
  - **SLE_12.SP0.PSX.load**
    - Editable script that mounts the iso, copies the rpms to local repositories in preparation for install and deployment

Installation example (SMW 8.0/CLE 6.0)



SLE_12.SP0.PS04 (glibc update)

smw:# **SLE_12.SP0.PS04.load**

- Site can modify this script to make local changes
- Mounts the iso as /media/SLES_12.SP0.PS04
- Copies patchset to /var/adm/cray/release/patchsets
- Unmounts the iso
- Runs record.patchset

Example

- **Updating SMW**

1. smw# **snaputil create __snapshot_backup_name__**
   - Allows backing out of problematic issues, safety first!
2. smw# **zypper update --dry-run**
   - See what zypper will do without affecting running system
3. smw# **zypper update**
   - Update the rpms in the currently running snapshot

Example

- **Updating CLE**

1. root@node# **zypper update**
   - Update a running node
2. smw# **imgbuilder**
   - Build new images with the updated rpms
   - Note no '--map'
3. smw# **cnode update --filter group=security_test -i …**
   - Boot the test node with the updated boot image

Future plans

Cray's OS Security team is new and still in transition.

It will be a continuing process to make improvements

Future plans may include:

- **Develop proactive approaches**
- **Scanners** – looking to understand sites' various scanners
  - Nessus vulnerability scanner
  - OpenSCAP
  - OSSEC
- **Tracking IAVA's in parallel with sites**
  - Potentially helpful in providing quicker responses and reducing surprises
  - Potential mechanism to map IAVA's to CVE's for better distro results

Summary

Provide security updates for all Cray products in a standardized process, on a planned schedule, allowing for priority issues to be handled in an expedited manner.

- Changes in the install process for newer products allow the flexibility for sites to deal with security updates while minimizing downtime.
- New Security team standardizing process among products.

Things to keep in mind

- **Make sure your entry in the online configuration database maintained by Cray field personnel is up to date.**
  - It's where we get the information to plan the builds of any Cray-built rpms for critical security updates.
  - If your entry is out of date, your patch may be delayed.

Things to keep in mind

- **General security inquiries, questions, advice**
  - Email os_security@cray.com

- **Birds of a Feather, Wednesday 5:15**
  - Vulnerability counts
  - SLES/CentOS lifecycle schedules

Legal Disclaimer

Information in this document is provided in connection with Cray Inc. products. No license, express or implied, to any intellectual property rights is granted by this document.

Cray Inc. may make changes to specifications and product descriptions at any time, without notice.

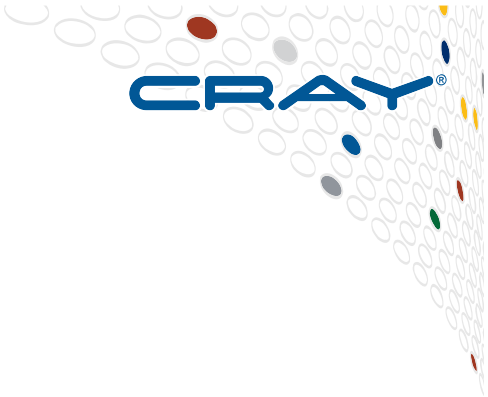
All products, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

Cray hardware and software products may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Cray uses codenames internally to identify products that are in development and not yet publically announced for release. Customers and other third parties are not authorized by Cray Inc. to use codenames in advertising, promotion or marketing and any use of Cray Inc. internal codenames is at the sole risk of the user.

Performance tests and ratings are measured using specific systems and/or components and reflect the approximate performance of Cray Inc. products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.

The following are trademarks of Cray Inc. and are registered in the United States and other countries: CRAY and design, SONEXION, and URIKA. The following are trademarks of Cray Inc.: APPRENTICE2, CHAPEL, CLUSTER CONNECT, CRAYPAT, CRAYPORT, ECOPHLEX, LIBSCI, NODEKARE, REVEAL, THREADSTORM. The following system family marks, and associated model number marks, are trademarks of Cray Inc.: CS, CX, XC, XE, XK, XMT, and XT. The registered trademark LINUX is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis. Other trademarks used in this document are the property of their respective owners.



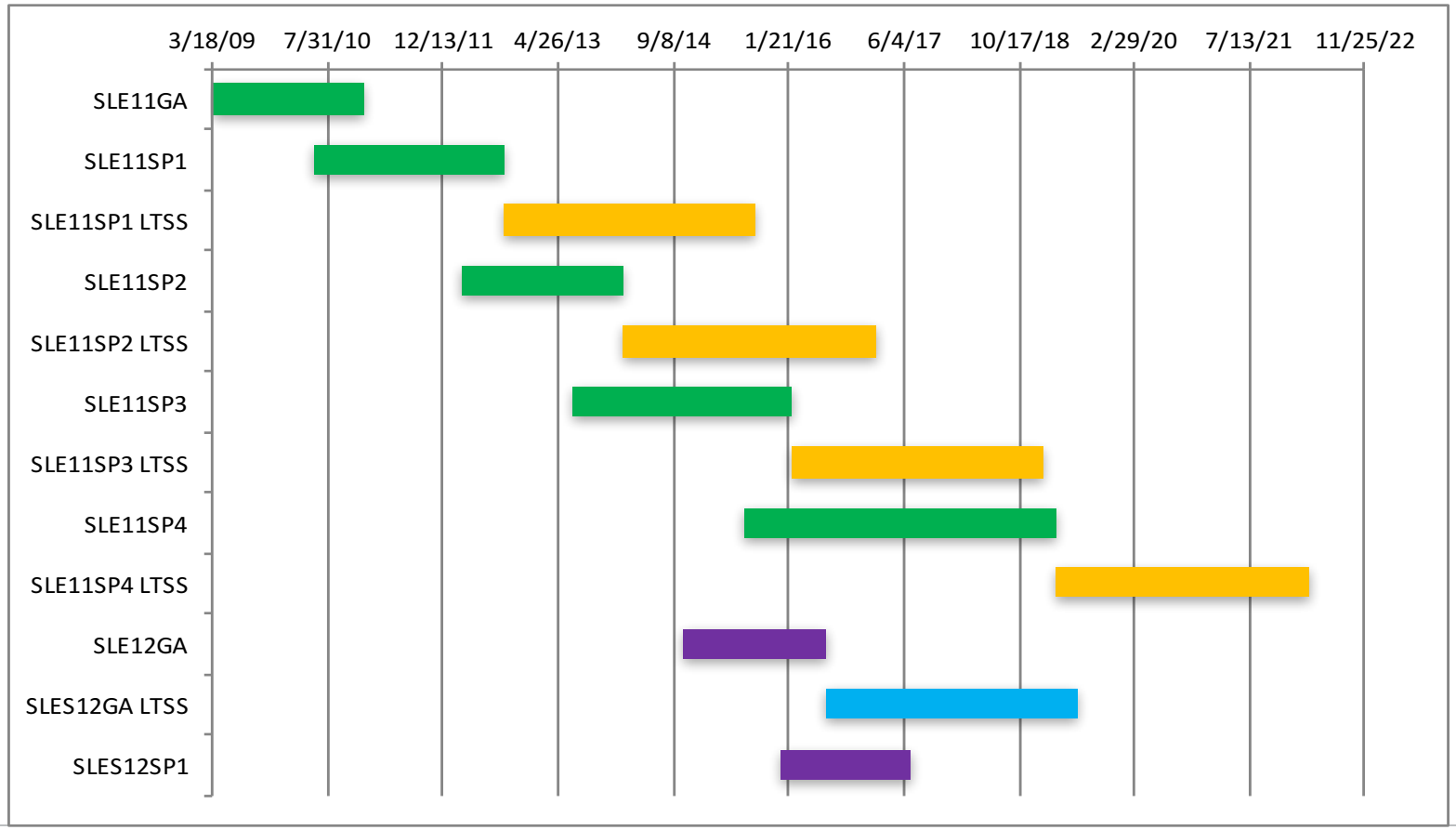
Q&A

Wendy Palm
wendy@cray.com
Technical information from Curt Fawcett & Luke Jacob

SUSE Lifecycle

- **Product supported for 10 years (*SLE11*)**
  - +3 years for extended support (LTSS), but may include only urgent/critical security updates
  - SLE11 released 24 Mar 2009, EOL 31 Mar 2019 (LTSS 2022) (CLE 3)
  - SLE12 released 27 Oct 2014, EOL 1 Oct 2021 (LTSS 2024) (CLE 6)
- **Service packs released every 18 months (*SLE11SP1, SP2, etc*)**
  - Service packs are supported for 6 months past the release of the next service pack
  - +3 years for extended support (LTSS), but may include only urgent/critical security updates
  - SLE 11SP1 released 20 June 2010, EOL 31 Aug 2012 (CLE 4)
  - SLE 11SP2 released 29 Feb 2012, EOL 31 Jan 2014 (CLE 5.0/5.1)
  - SLE 11SP3 released 31 Jan 2013, EOL 31 Jan 2016 (CLE 5.2)
  - SLE 11SP4 released 15 Jul 2015, EOL 31 Mar 2019
- **When support ends, Cray cannot get further updates**

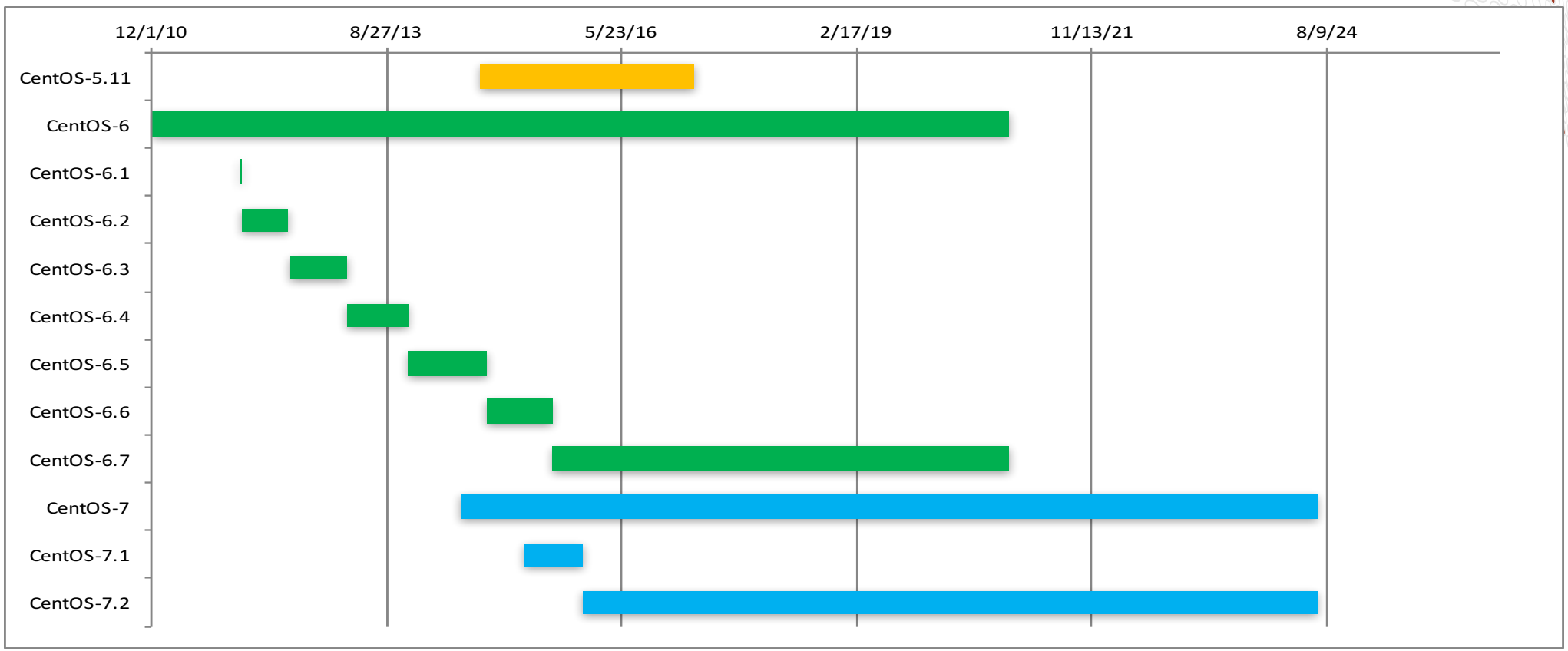
SLE Lifecycle



CentOS Lifecycle

- **Major release supported for 10 years (*CentOS6*)**
  - CentOS-6 released 1 Dec 2010, EOL 30 Nov 2020
  - CentOS-7 released 1 Jul 2014, EOL 30 Jun 2024
- **Minor releases released ~every 10mos (*CentOS-6.7*)**
  - CentOS-6.6 released 28 Oct 2014, EOL 6 Aug 2015
  - CentOS-6.7 released 7 Aug 2015
  - CentOS-7.1 released 2 Apr 2015, EOL 13 Dec 2015
  - CentOS-7.2 released 14 Dec 2015
- **Active support for each release moves to the next release; support is not available for older releases (both Major and Minor).**

CentOS Lifecycle



By the numbers - SLES9

- **SLES9 – released 8/03/2004, ended maint 8/31/2011**

  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-packagemanger-devel, km_nss, openssl, samba, tk, pcre.

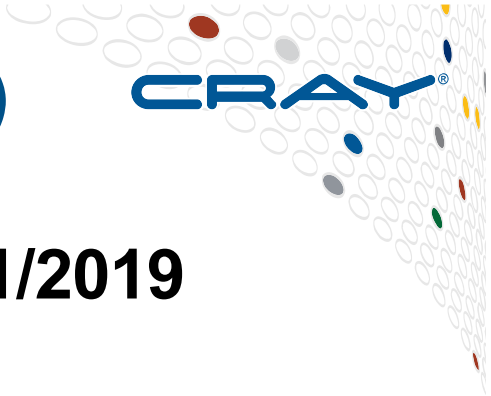
- **SMW 1.5/3.1 & Unicos/lc 1.5/2.0**
  - 948 rpms in dist
  - 54 FNs, 965 updates of 255 rpms, 511 CVEs

- **XD1**
  - 1420 rpms in dist (pretty much all of them)
  - 29 FNs, 1544 updates of 292 rpms, 670 CVEs

By the numbers – SLES10

- **SLES10 – released 7/17/2006, end maint 7/31/2013**
- **SMW 3.1.10/4.0 & CLE 2.1/2.2**
  - 1084 rpms in SMW dist
  - 1299 rpms in CLE 2.1 dist
  - 1025 rpms in CLE 2.2 dist (rpmreduction project)
- **48 FNs, 1812 updates of 380 rpms, 1162 CVEs**

By the numbers – SLES11 (as of 3/23/2016)



- **SLES11 – released 3/24/2009, end maint 1/31/2019**
- **SMW 5/6/7 & CLE 3/4/5**
  - Novell re-organized their rpms – many broke into multiple rpms and many devel rpms got moved into SDK & SLED.
  - 1225 rpms in SMW dist
  - 1788 rpms in CLE dist
  - 1112 rpms in ESMS dist
- **72 FNs, 2415 updates of 637 rpms, 2367 CVEs**

Relevant Security Vulnerabilities