

Linux Kernel Release Model

(and security stuff)

Greg Kroah-Hartman
gregkh@linuxfoundation.org

github.com/gregkh/presentation-release-model

69,300 files
28,995,000 lines

4,645 developers
450+ companies

8,900 lines added
2,700 lines removed
2,100 lines modified

8,900 lines added

2,700 lines removed

2,100 lines modified

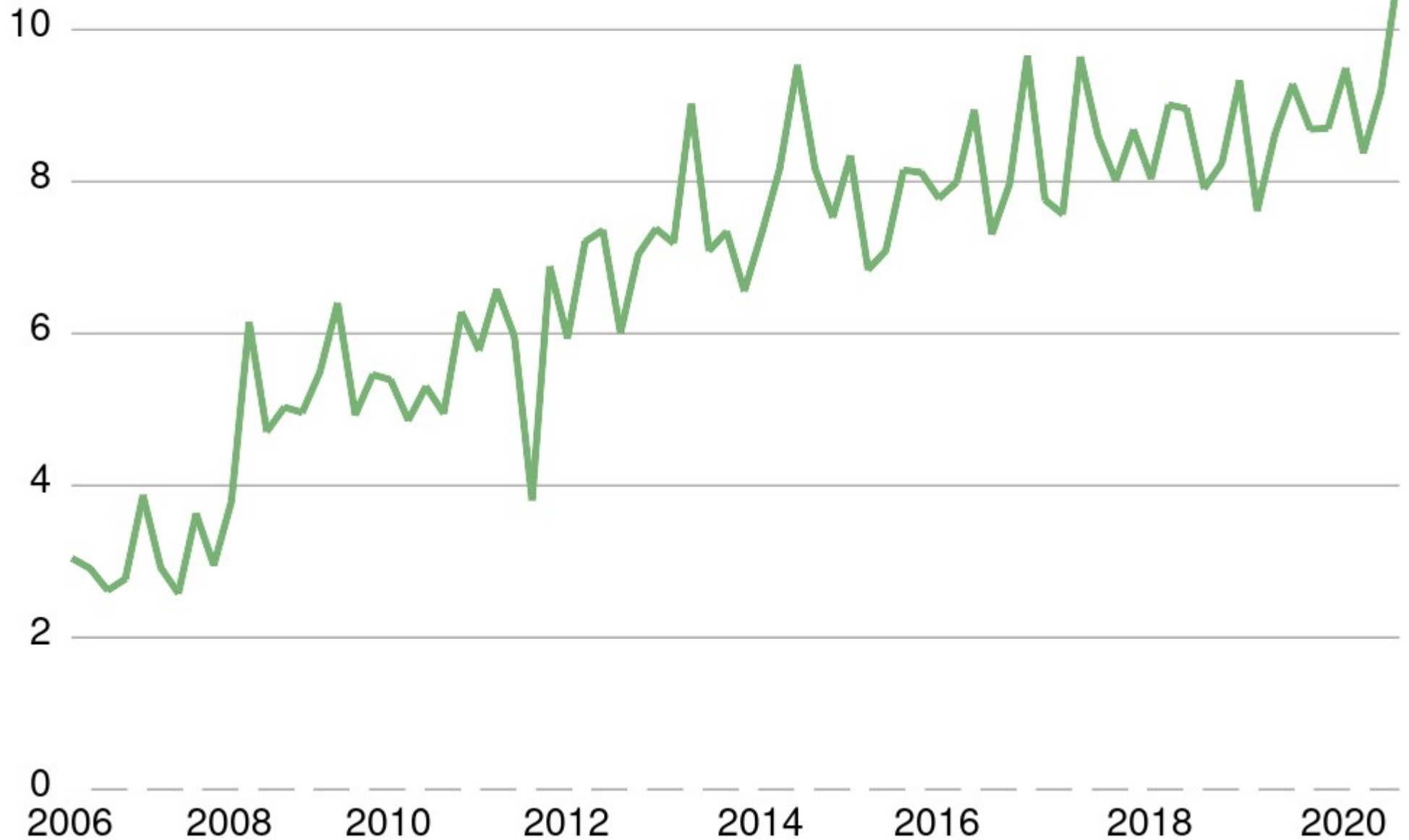
Every day

9.2 changes per hour

10.8 changes per hour

5.8 release

Patches merged per hour



Old release model

2.2 – January 1999

2.4 – January 2001

2.6 – December 2003

“New” release model

Release every 2-3 months

All releases are stable

“Cambridge Promise”

Will not break userspace.

“Cambridge Promise”

Will not break userspace,
on purpose.

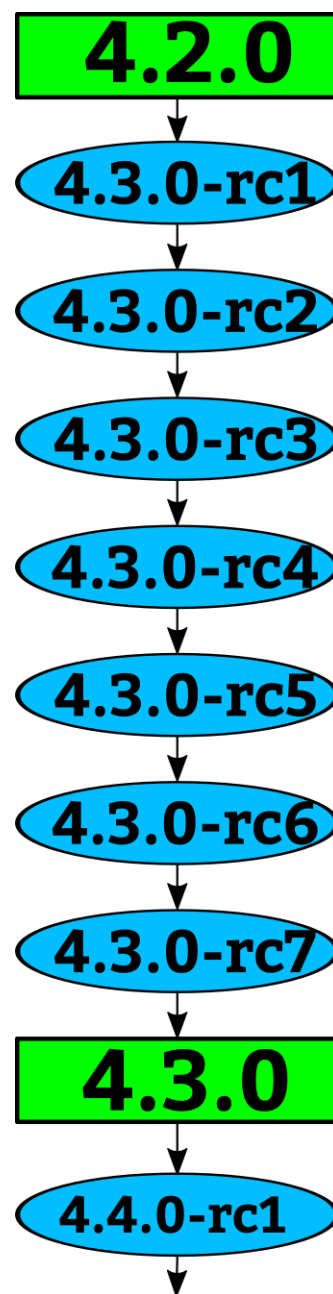
– July 2007

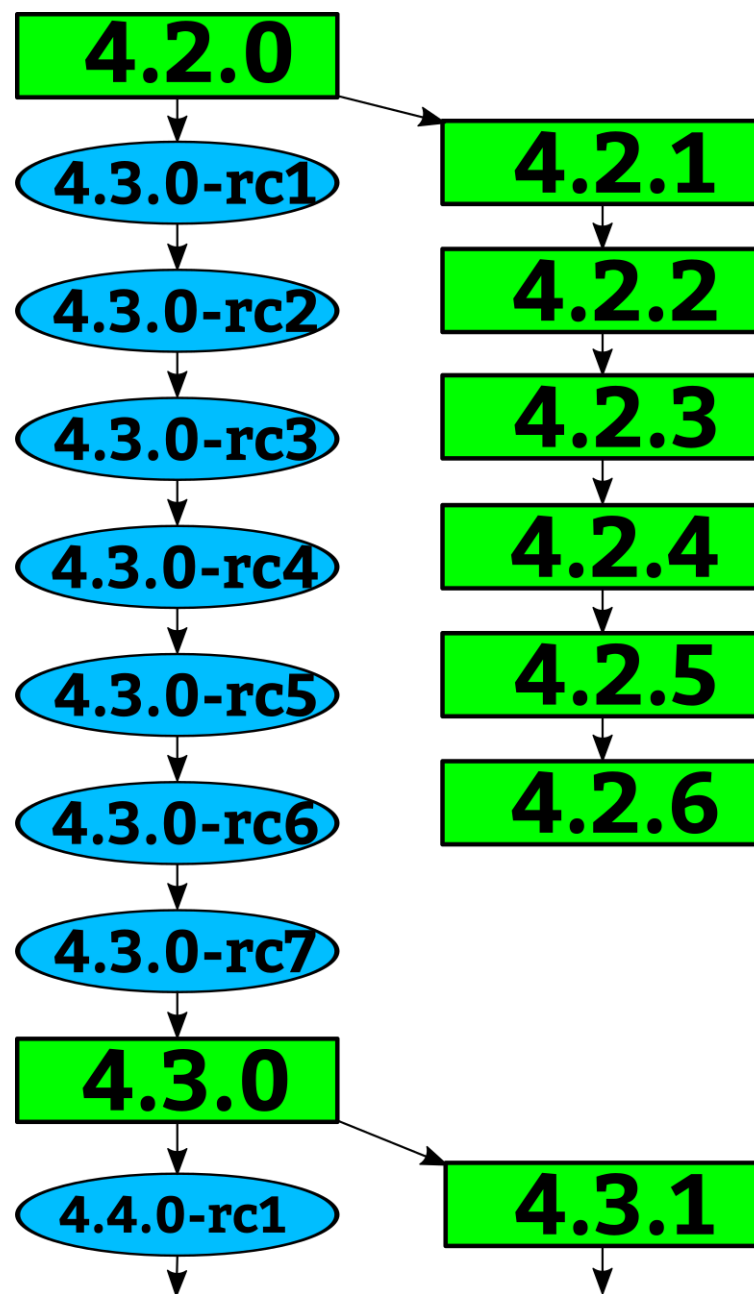
Version numbers
mean nothing

2.6.x → 3.x 2011

$3.x \rightarrow 4.x$ 2015

4.x \rightarrow 5.x 2019





Stable rules

- Bugfix
- Less than 100 lines
- New ids or quirks
- Must be in Linus's tree

kernel.org/doc/html/latest/process/stable-kernel-rules.html

“Longterm kernels”

One picked per year

Maintained for at least 2 years

4.4 4.9 4.14 4.19 5.4

kernel.org/category/releases

4.4	9 changes / day
4.9	13 changes / day
4.14	18 changes / day
4.19	23 changes / day
5.4	28 changes / day
5.7	33 changes / day

Every release is stable

Decade old guarantee

Always update your kernel

Can't update your kernel?

Blame your SoC provider...

“Popular” SoC kernel tree

6171 files changed 2837180 insertions(+), 42568 deletions(-)

“Popular” SoC kernel tree

6171 files changed 2837180 insertions(+), 42568 deletions(-)

Image.lz4 – 3.2 million lines

Linux “like”

Kernel Security

Kernel Security

Almost all bugs can be a “security” issue.

Kernel Security

Almost all bugs can be a “security” issue.

Fix them as soon as possible.

Kernel Security

Almost all bugs can be a “security” issue.

Fix them as soon as possible.

[How the Kernel Security team works](#)

Linux security fixes

- Happen at least once a week
- Look like any other bugfix
- Rarely called out as a security fix
- Most fixes not known to be security related until much later
- Very few CVEs ever get assigned

Linux security fixes \neq CVEs

- Small fraction of kernel fixes get CVEs
- Cherry-picking CVEs result in insecure system
- Some CVEs have follow-on fixes not listed

Linux security fixes \neq CVEs

- Small fraction of kernel fixes get CVEs
- 2006-2018 had 1005 CVEs for Linux
 - 41% (414) had negative “fix date”
 - 12 never fixed
 - Average fix date, -100 days
 - Longest fix dates, -3897 and 2348
 - 88 fixed within 1 week
 - Standard deviation 405 days

CVEs mean nothing for Linux

[More details](#) for the curious

Linux Longterm kernels fix problems

- Bugs are fixed before you realize it
- Google security team requests in 2018:
 - 92% (201/218) problems already fixed in LTS release
 - No need for cherry-picking
 - Remaining issues were due to out-of-tree code

Linux Longterm kernels fix problems

- Bugs are fixed before you realize it
- Google security team requests in 2019:
 - 90% problems already fixed in LTS release
 - 950+ critical non-security bugs also fixed

Linux Longterm kernels fix problems

Android now requires LTS kernel updates

Keeping a Secure System

Take **all** stable kernel updates

Enable hardening features

“If you are not using a stable /
longterm kernel, your system
is insecure”

– me



github.com/gregkh/presentation-release-model

