Samba and the AI security tsunami

Douglas Bagnall, Catalyst IT and Samba team

Less specific than originally planned

a couple of weeks ago:

the security release that was scheduled for tomorrow, will be postponed due to new problems that have been identified with one of the fixes.

Strong belief in AI efficacy is not necessary

With this level of investment, psychic octopuses would find bugs

Strong belief in AI efficacy is not necessary

With this level of investment, psychic octopuses would find bugs

1. report security bugs in Samba!
2. ???
3. profit!!

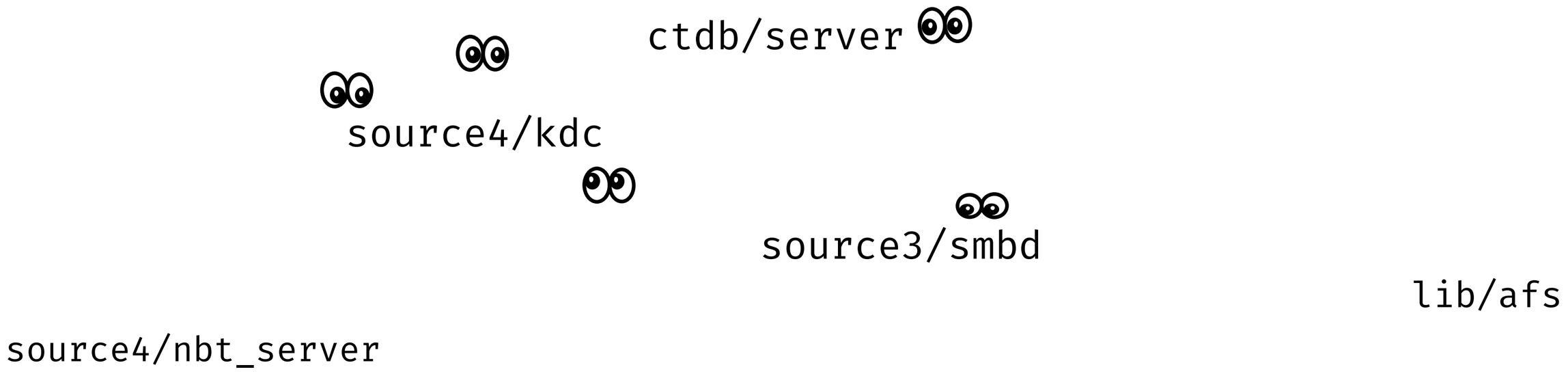
Strong belief in AI efficacy is not necessary

With this level of investment, psychic octopuses would find bugs

1. report security bugs in Samba!
2. *pay us to do this to your code before evildoers do*
3. profit!!

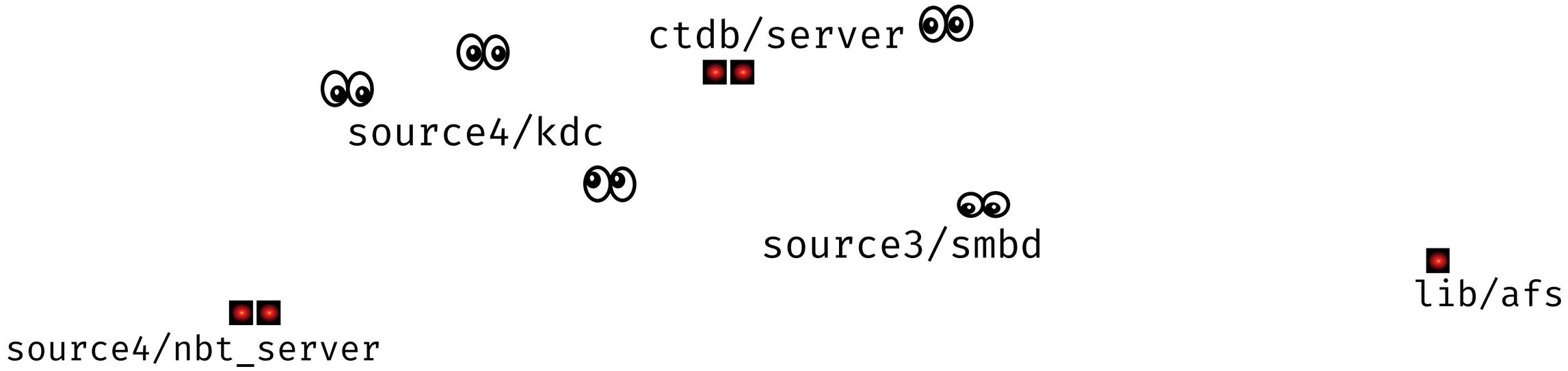
“given enough eyeballs, all bugs are shallow”

Never convincing, since our eyes that know where not to look



“given enough eyeballs, all bugs are shallow”

Never convincing, since our eyes that know where not to look



Reports up until March 2026

About eight unique valid reports
about four duplicate reports
about four invalid reports

Reports up until March 2026

About eight unique valid reports
about four duplicate reports
about four invalid reports

https://bugzilla.samba.org/show_bug.cgi?id=15918
took hours to discover it wasn't reachable

Reports up until March 2026

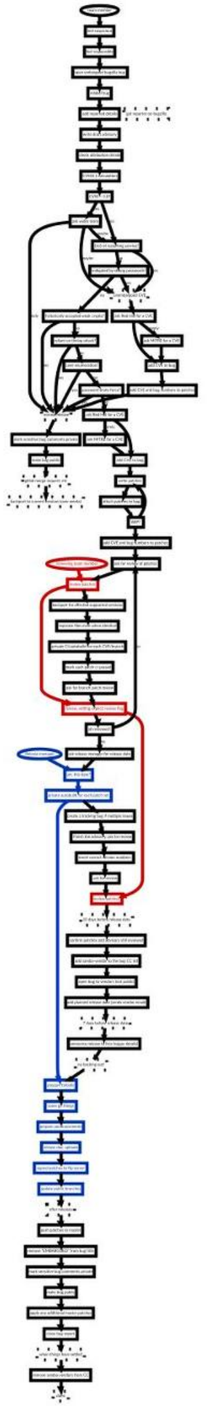
About eight unique valid reports
about four duplicate reports
about four invalid reports

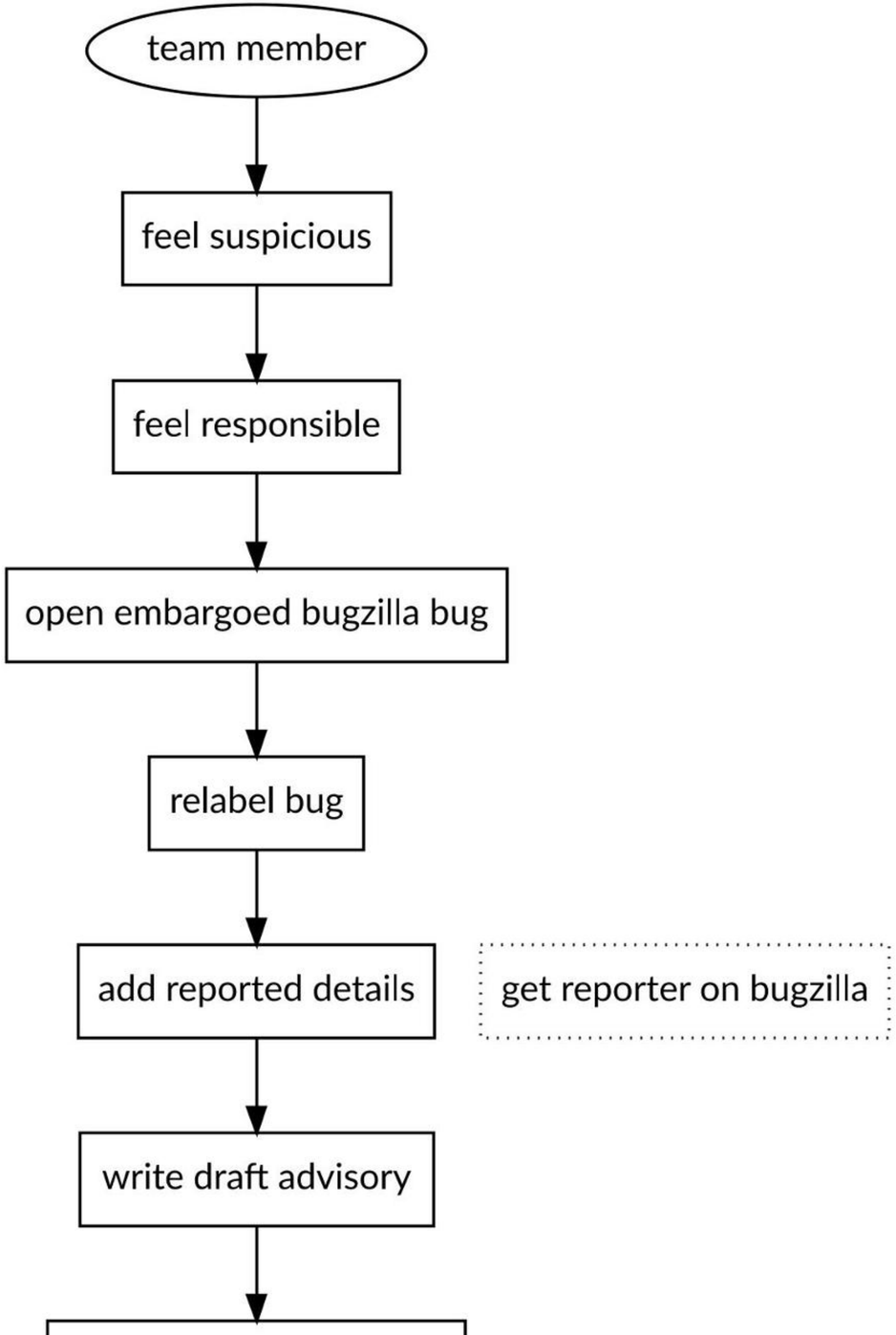
https://bugzilla.samba.org/show_bug.cgi?id=15918
took hours to discover it wasn't reachable

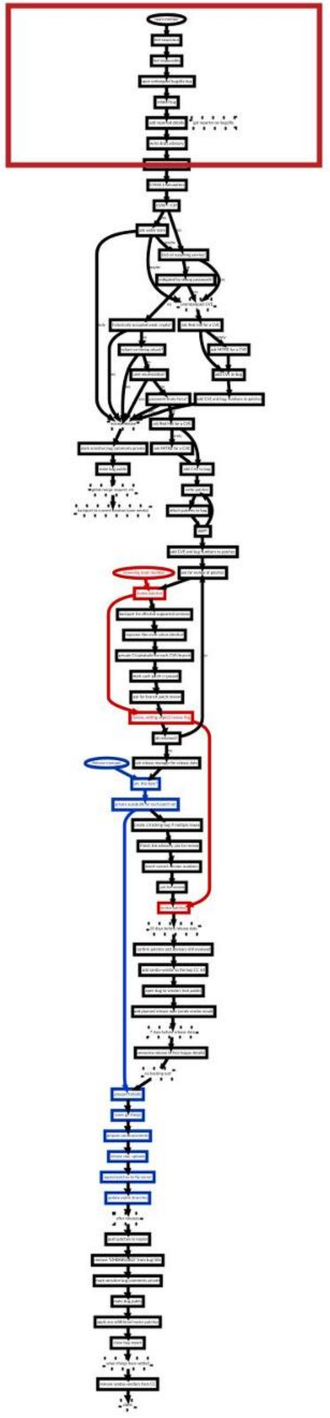
<h@ckor> I copy samba code into threads, and it breaks!
<volker> why would you do that?
<h@ckor> ... sorry, bye

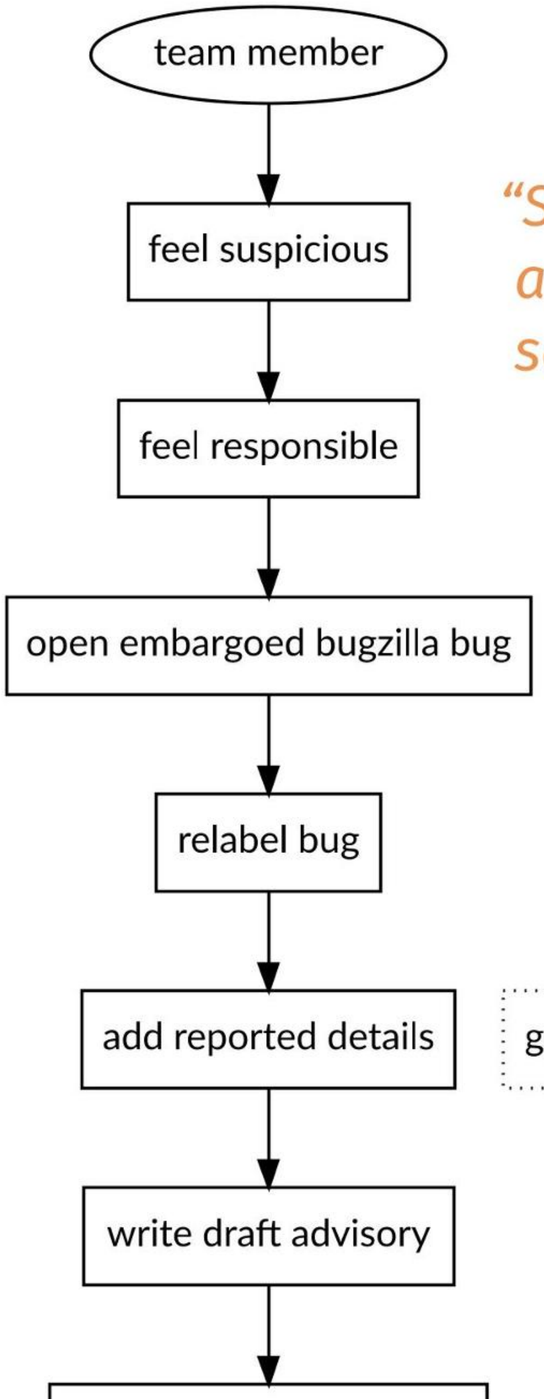
Security release process

https://wiki.samba.org/index.php/Samba_Security_Process



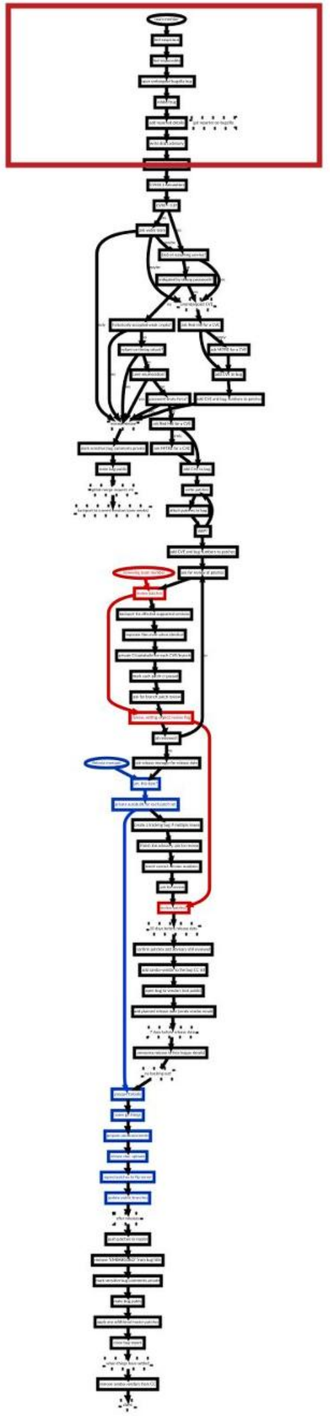

team member
feel suspicious
feel responsible
open embargoed bugzilla bug
relabel bug
add reported details
get reporter on bugzilla
write draft advisory

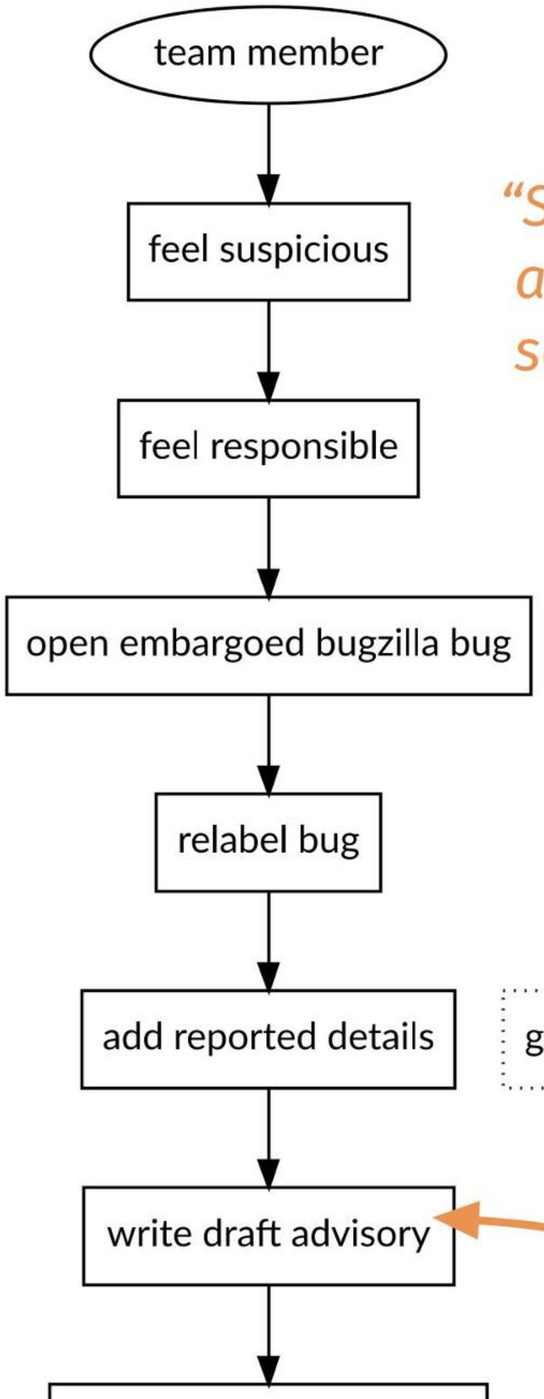




"Someone should feel responsible and make sure that it's really a security defect."

get reporter on bugzilla

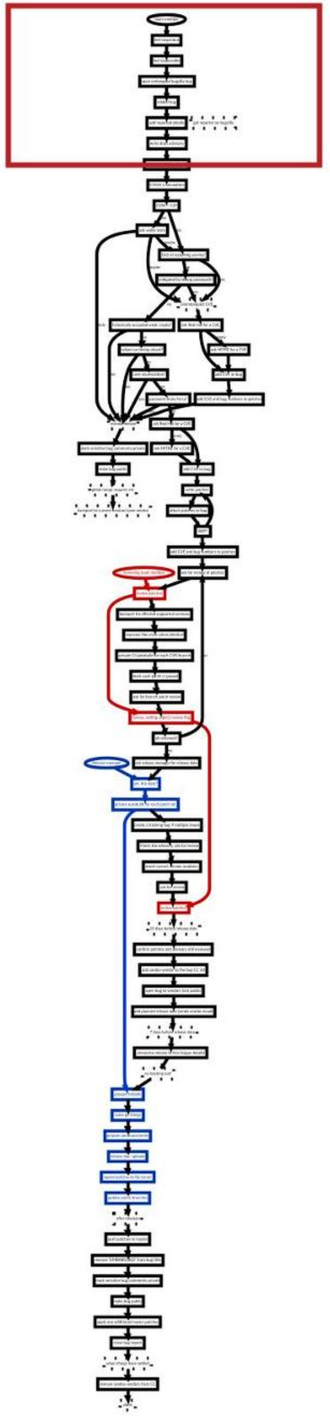


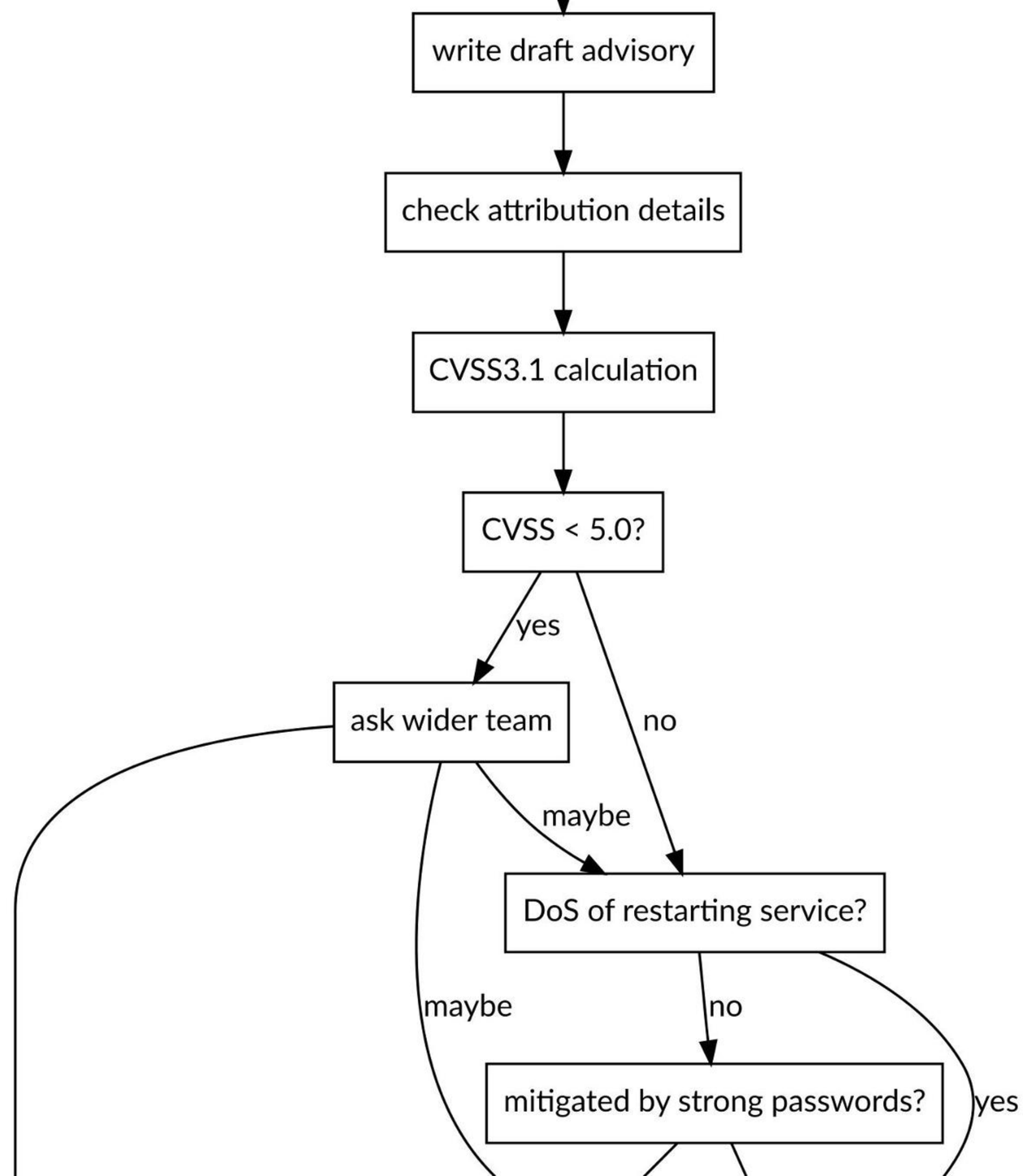


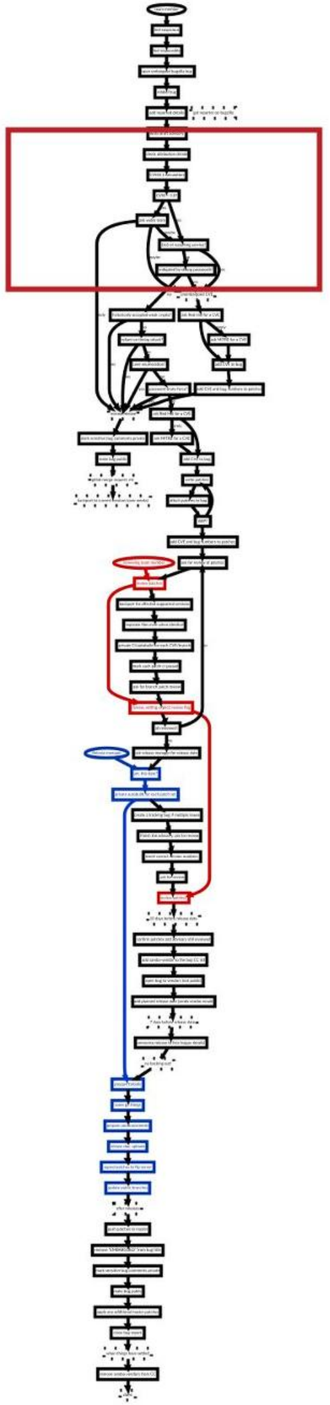
"Someone should feel responsible and make sure that it's really a security defect."

sometimes difficult

often left till later




write draft advisory
check attribution details
CVSS3.1 calculation
CVSS < 5.0?
yes
no
ask wider team
maybe
DoS of restarting service?
maybe
no
mitigated by strong passwords?
yes



write draft advisory

check attribution details

CVSS3.1 calculation

interpretations sometimes differ

CVSS < 5.0?

yes

no

ask wider team

maybe

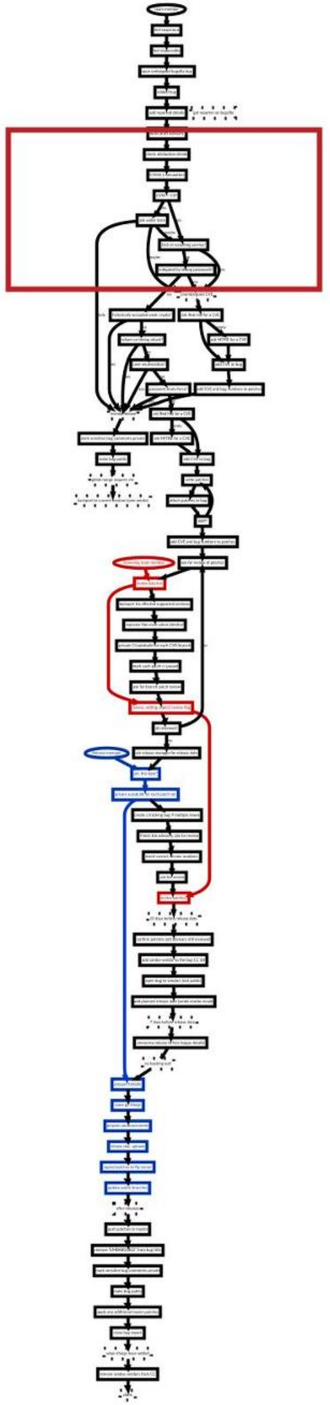
DoS of restarting service?

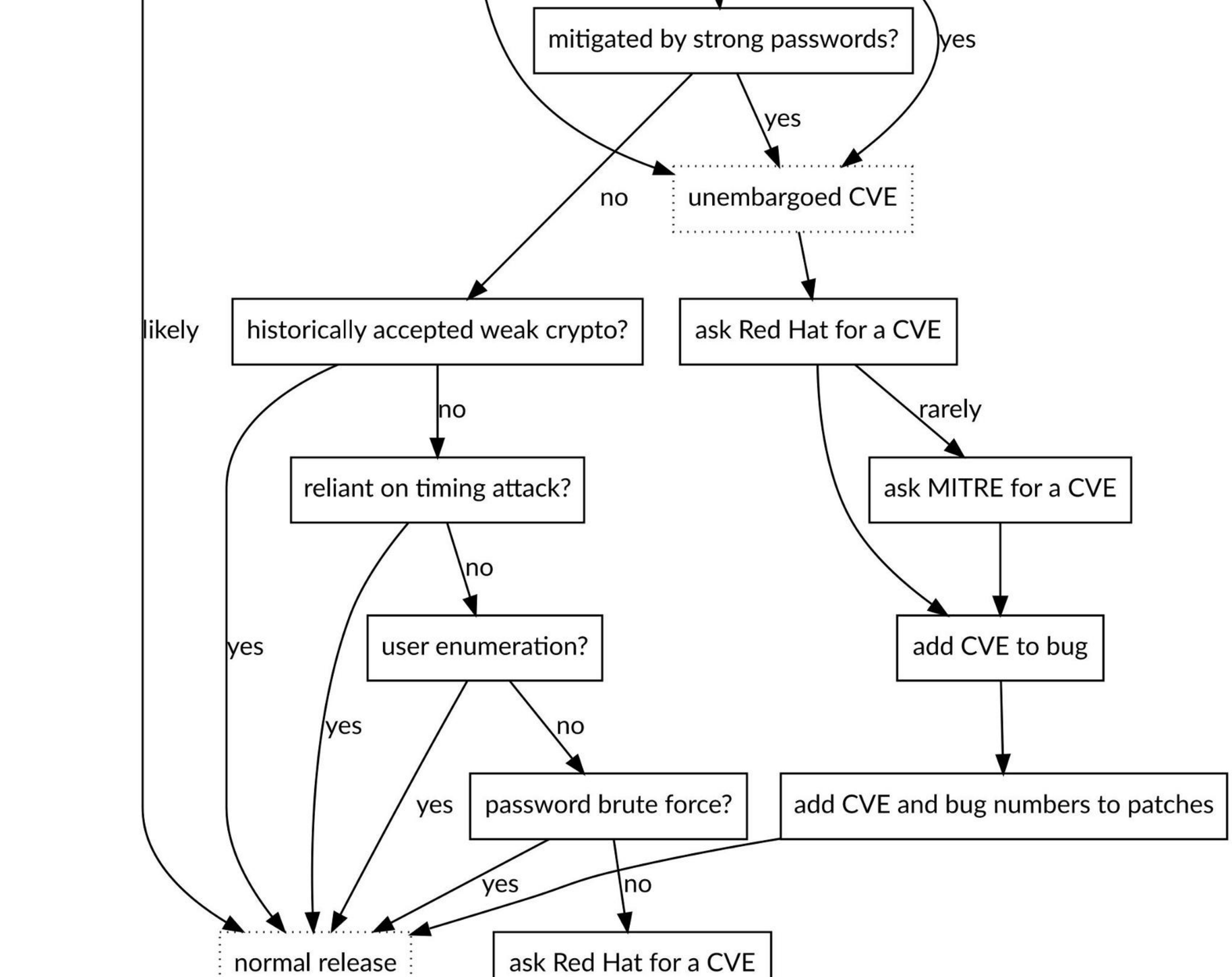
maybe

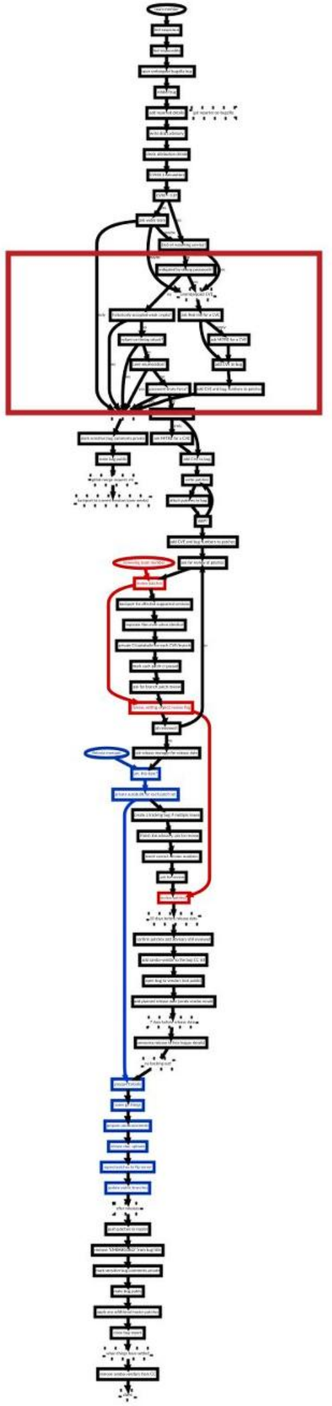
no

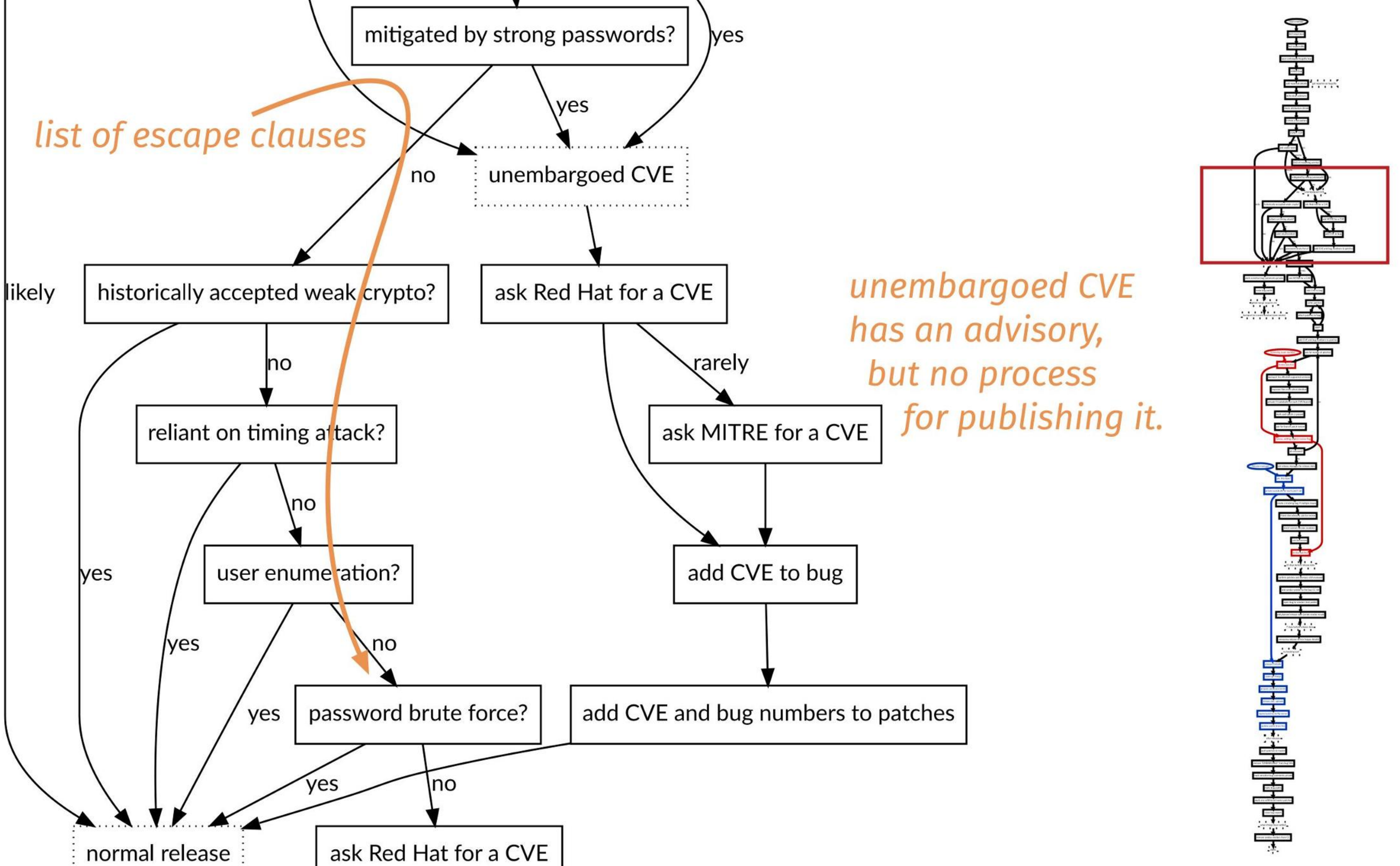
mitigated by strong passwords?

yes




mitigated by strong passwords?
yes
yes
no
unembargoed CVE
likely
historically accepted weak crypto?
ask Red Hat for a CVE
no
rarely
reliant on timing attack?
ask MITRE for a CVE
no
yes
user enumeration?
add CVE to bug
yes
no
yes
password brute force?
add CVE and bug numbers to patches
yes
no
normal release
ask Red Hat for a CVE




mitigated by strong passwords?
yes
yes
list of escape clauses
no
unembargoed CVE
likely
historically accepted weak crypto?
ask Red Hat for a CVE
unembargoed CVE
has an advisory,
but no process
for publishing it.
no
rarely
reliant on timing attack?
ask MITRE for a CVE
no
yes
user enumeration?
add CVE to bug
yes
no
yes
password brute force?
add CVE and bug numbers to patches
yes
no
normal release
ask Red Hat for a CVE

normal release

ask Red Hat for a CVE

rarely

mark sensitive bug comments private

ask MITRE for a CVE

make bug public

add CVE to bug

gitlab merge request, etc

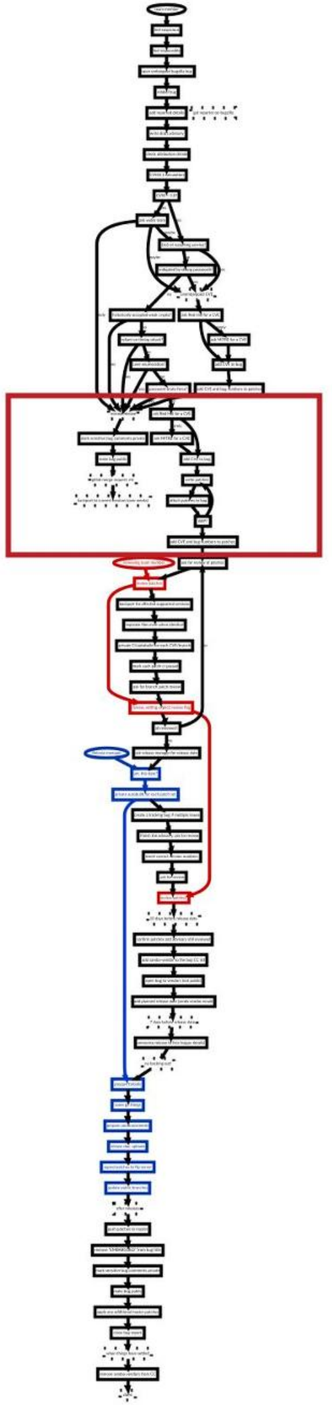
write patches

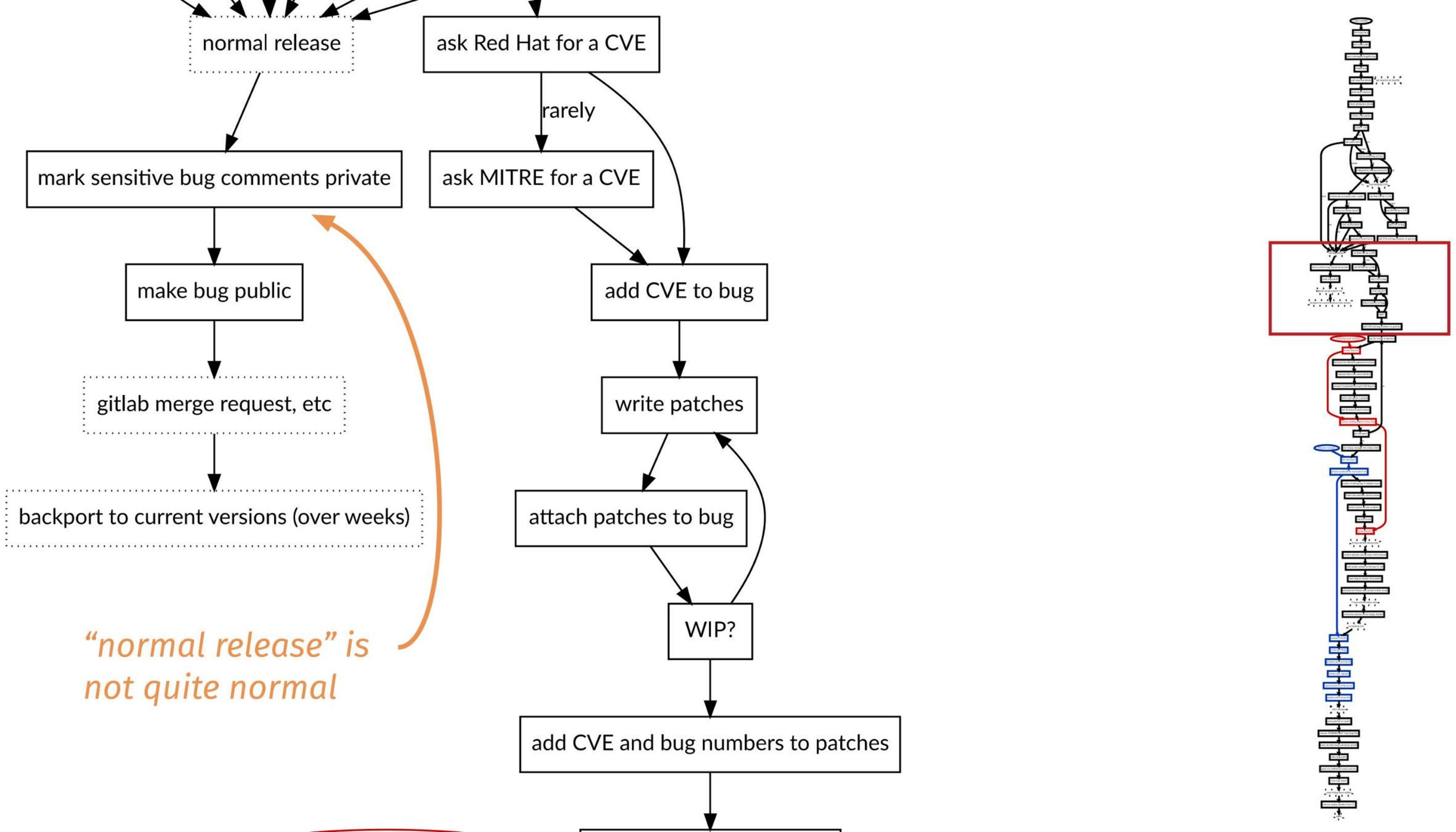
backport to current versions (over weeks)

attach patches to bug

WIP?

add CVE and bug numbers to patches




normal release
ask Red Hat for a CVE
rarely
mark sensitive bug comments private
ask MITRE for a CVE
make bug public
add CVE to bug
gitlab merge request, etc
write patches
backport to current versions (over weeks)
attach patches to bug
WIP?
add CVE and bug numbers to patches
“normal release” is not quite normal

add CVE and bug numbers to patches

reviewing team member

ask for review of patches

review patches

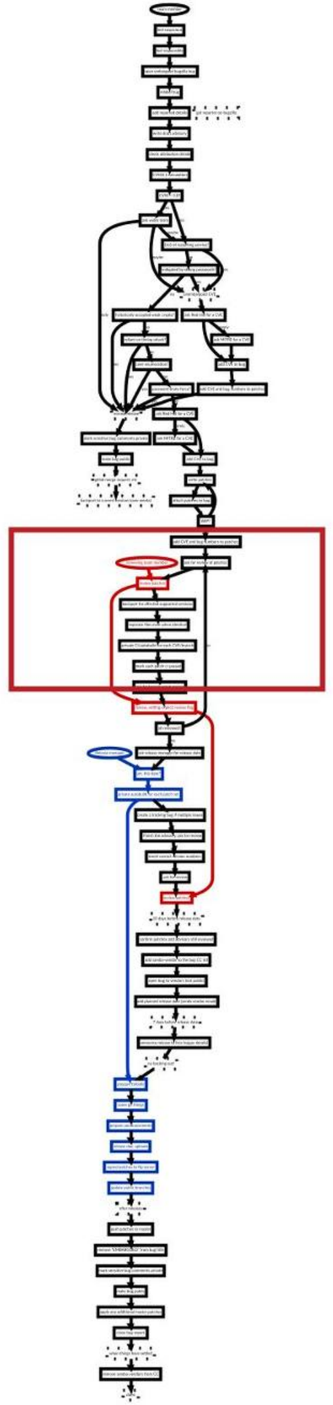
backport for affected supported versions

separate files even when identical

private CI/autobuild for each CVE/branch

no

mark each patch ci-passed



add CVE and bug numbers to patches

reviewing team member

ask for review of patches

review patches

backport for affected supported versions

separate files even when identical

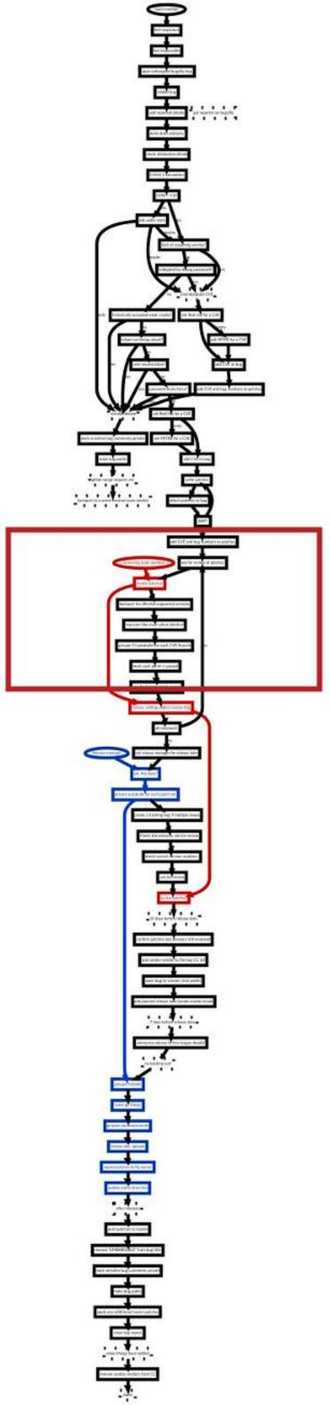
private CI/autobuild for each CVE/branch

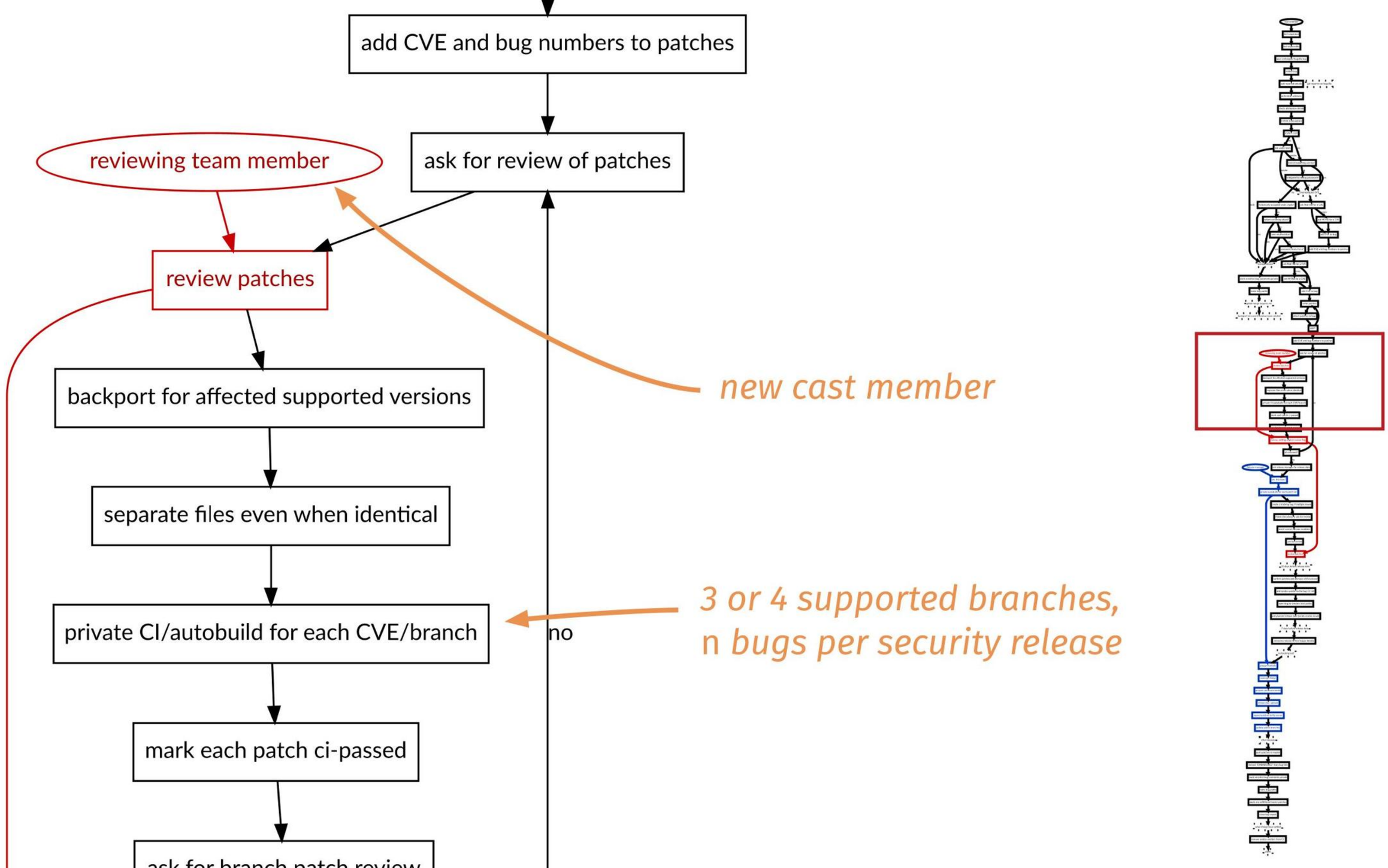
mark each patch ci-passed

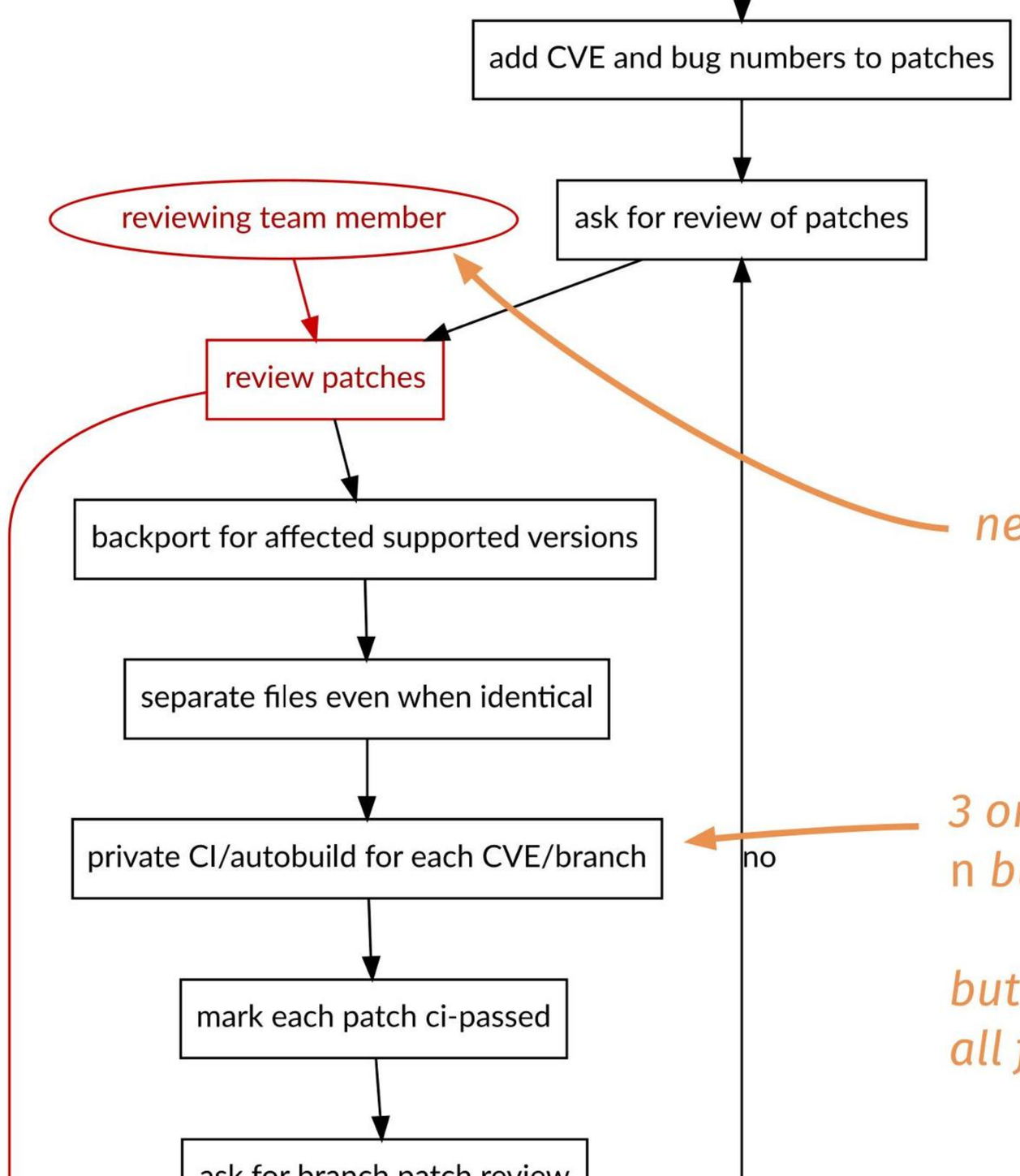
ask for branch patch review

no

new cast member



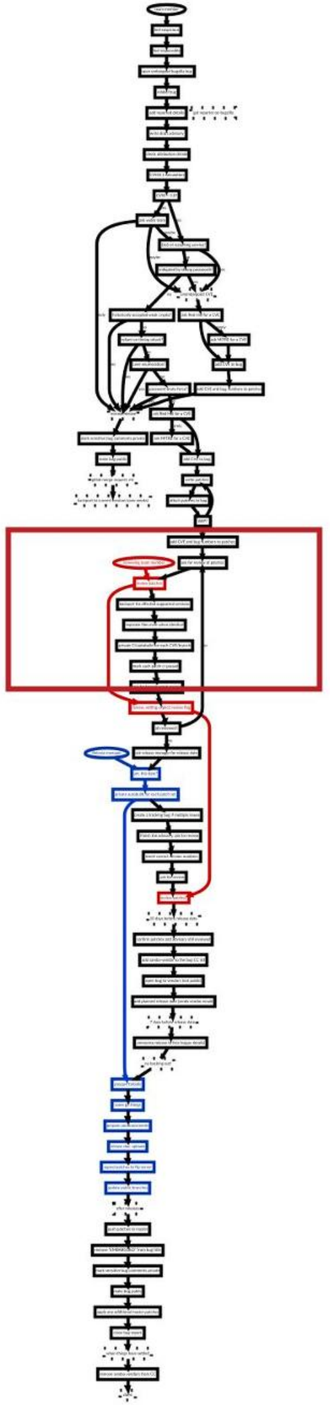

add CVE and bug numbers to patches
ask for review of patches
reviewing team member
review patches
backport for affected supported versions
separate files even when identical
private CI/autobuild for each CVE/branch
mark each patch ci-passed
ask for branch patch review
no
new cast member
3 or 4 supported branches,
n bugs per security release

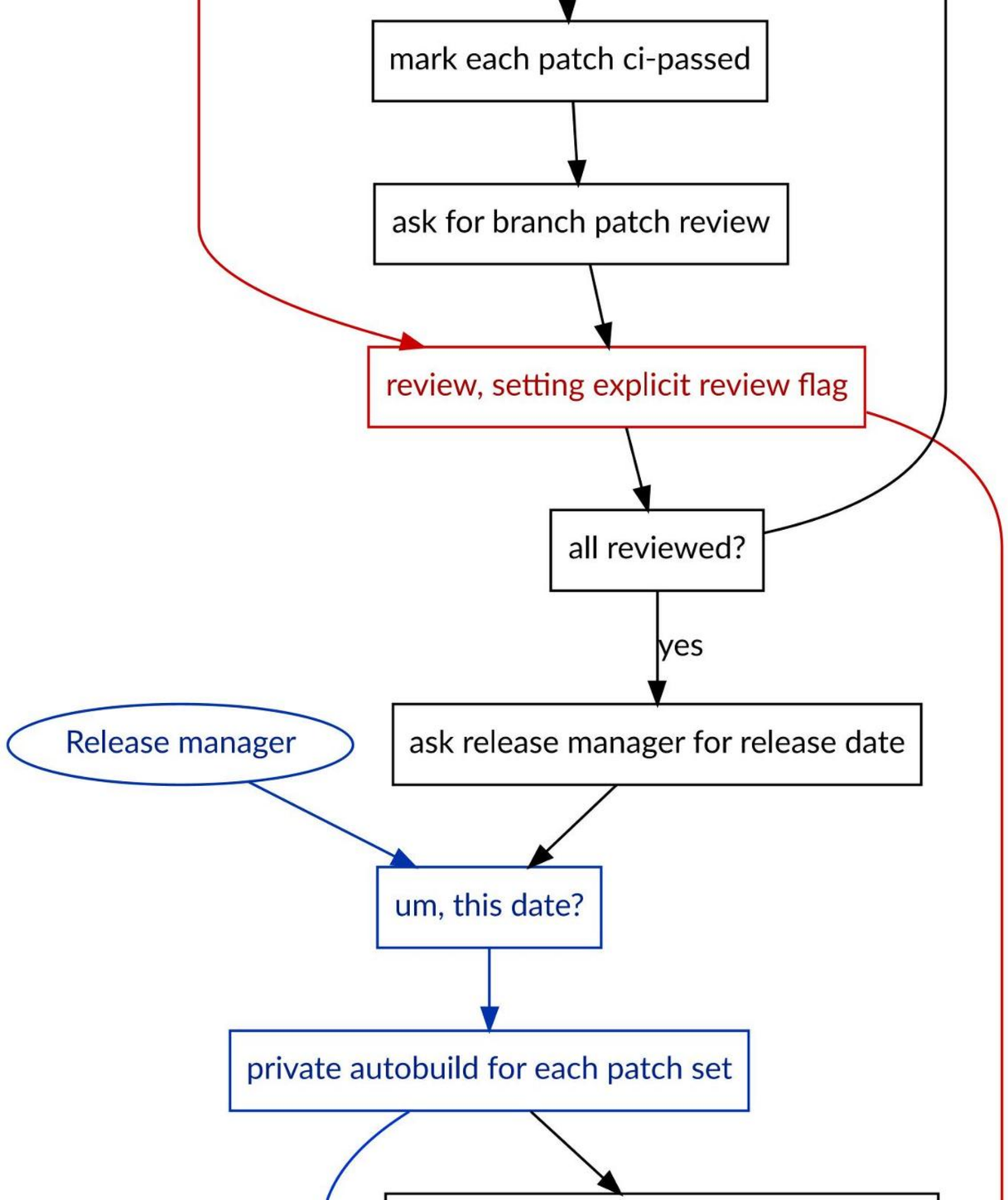


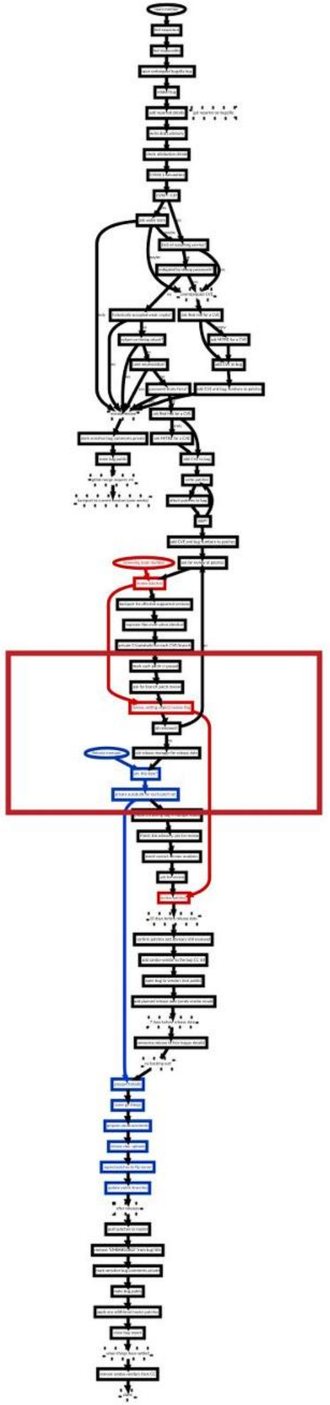
new cast member

3 or 4 supported branches,
n bugs per security release

but we really only care about
all fixes in combination




mark each patch ci-passed
ask for branch patch review
review, setting explicit review flag
all reviewed?
yes
Release manager
ask release manager for release date
um, this date?
private autobuild for each patch set



mark each patch ci-passed

ask for branch patch review

review, setting explicit review flag

all reviewed?

yes

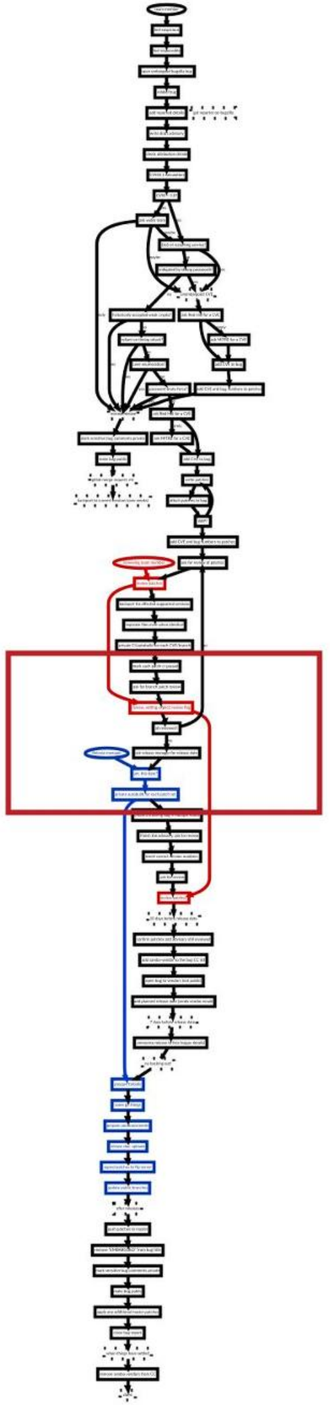
Release manager

ask release manager for release date

um, this date?

private autobuild for each patch set

Another new character



mark each patch ci-passed

ask for branch patch review

review, setting explicit review flag

all reviewed?

yes

Release manager

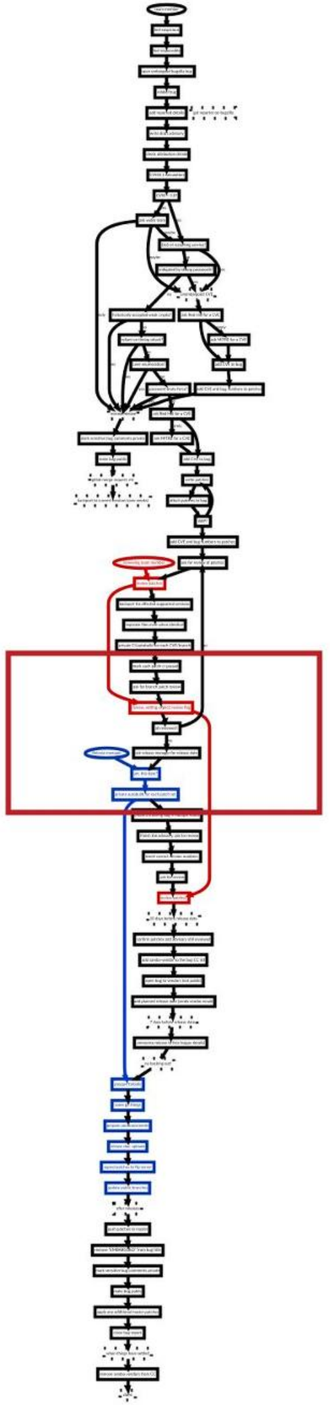
ask release manager for release date

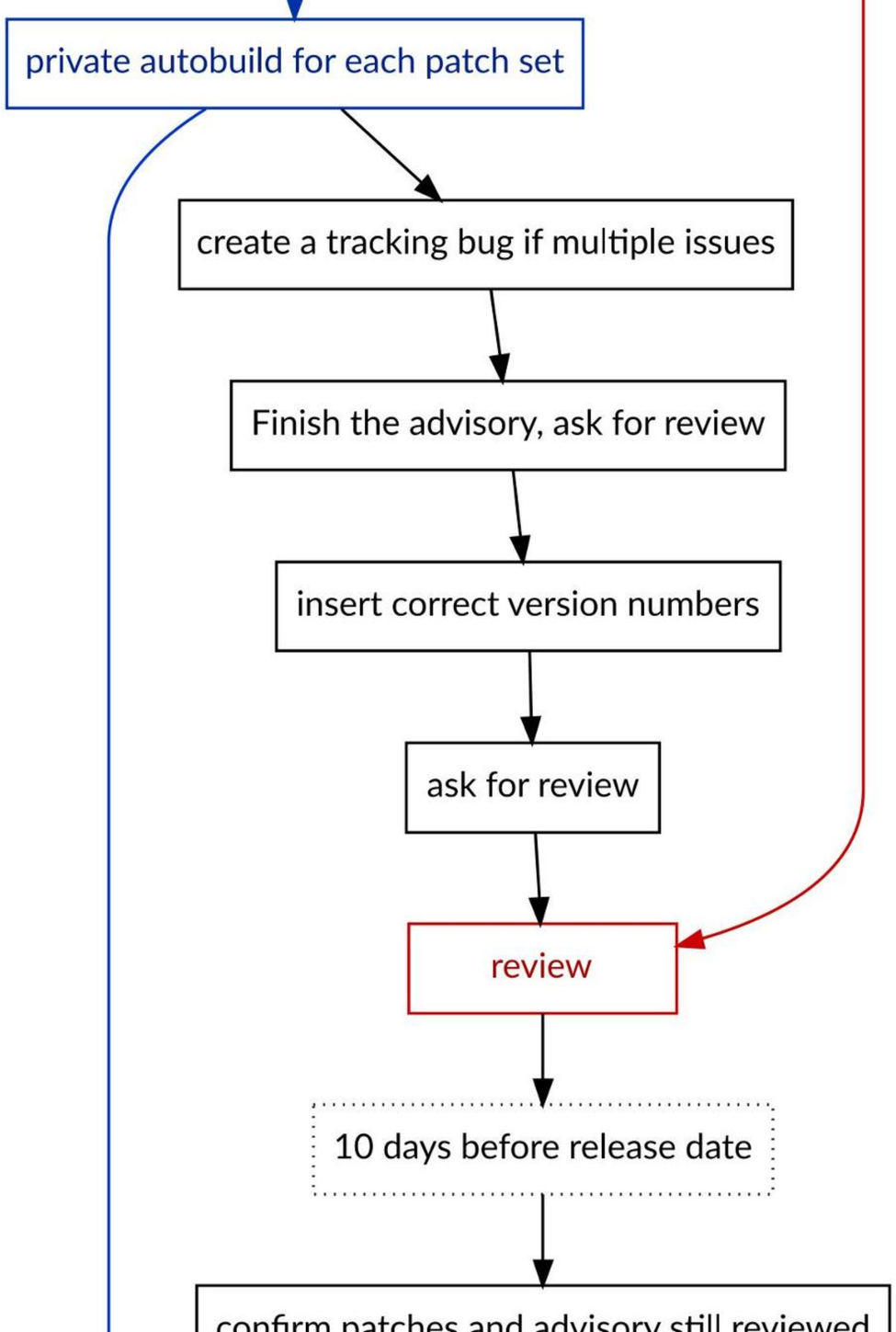
um, this date?

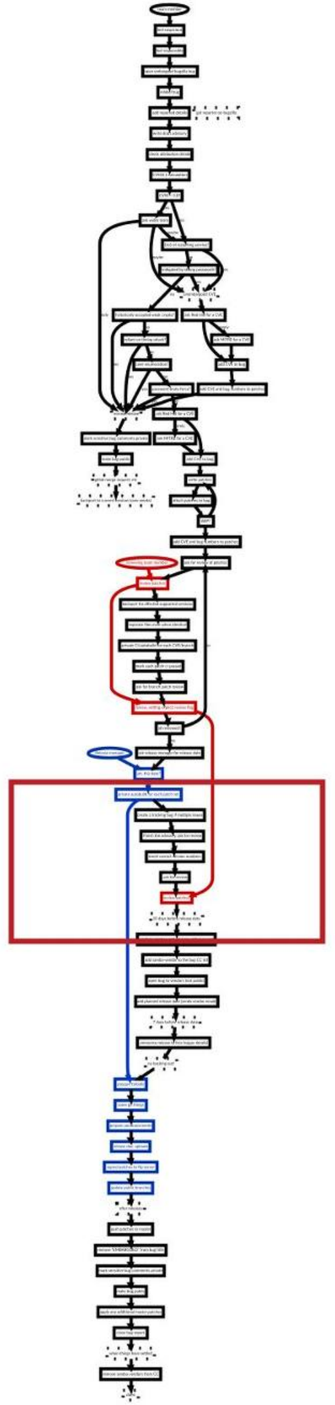
private autobuild for each patch set

Another new character

The test we care about




private autobuild for each patch set
create a tracking bug if multiple issues
Finish the advisory, ask for review
insert correct version numbers
ask for review
review
10 days before release date
confirm patches and advisory still reviewed



private autobuild for each patch set

create a tracking bug if multiple issues

Finish the advisory, ask for review

insert correct version numbers

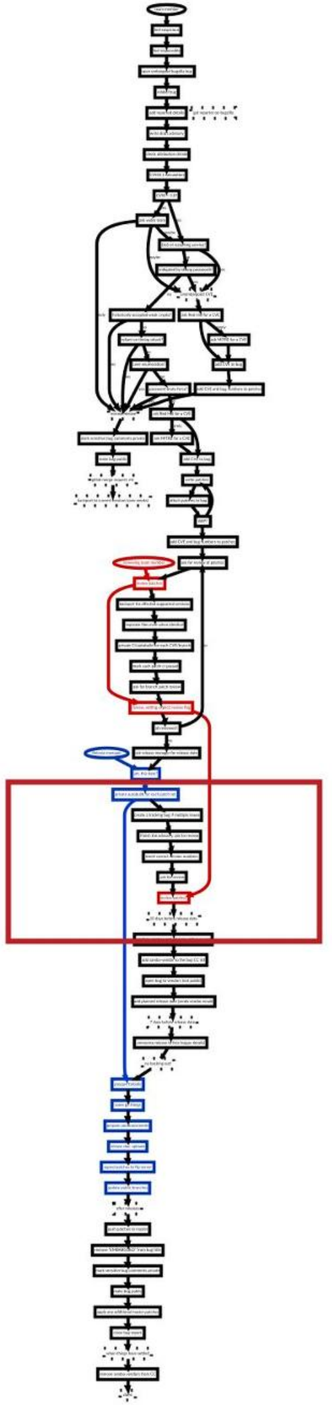
ask for review

review

10 days before release date

confirm patches and advisory still reviewed

would have been useful earlier



10 days before release date

confirm patches and advisory still reviewed

add samba-vendor to the bug CC list

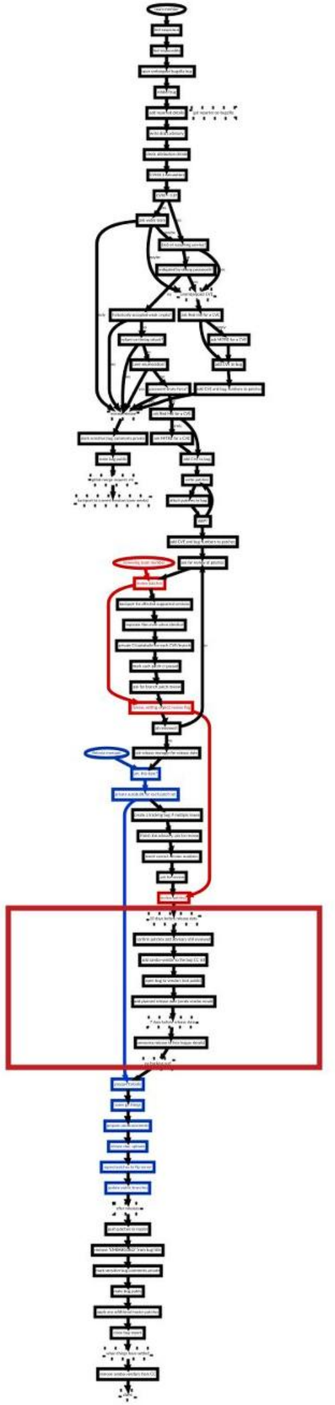
open bug to vendors (not public)

add planned release date (sends vendor email)

7 days before release date

announce release to lists (vague details)

no backing out!



10 days before release date

confirm patches and advisory still reviewed

add samba-vendor to the bug CC list

open bug to vendors (not public)

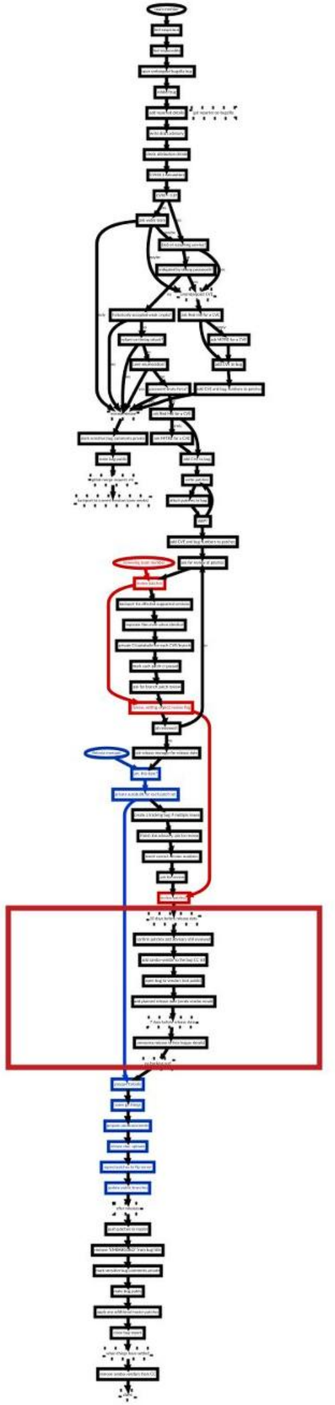
add planned release date (sends vendor email)

7 days before release date

announce release to lists (vague details)

no backing out!

There will be a security release on ...



10 days before release date

confirm patches and advisory still reviewed

add samba-vendor to the bug CC list

open bug to vendors (not public)

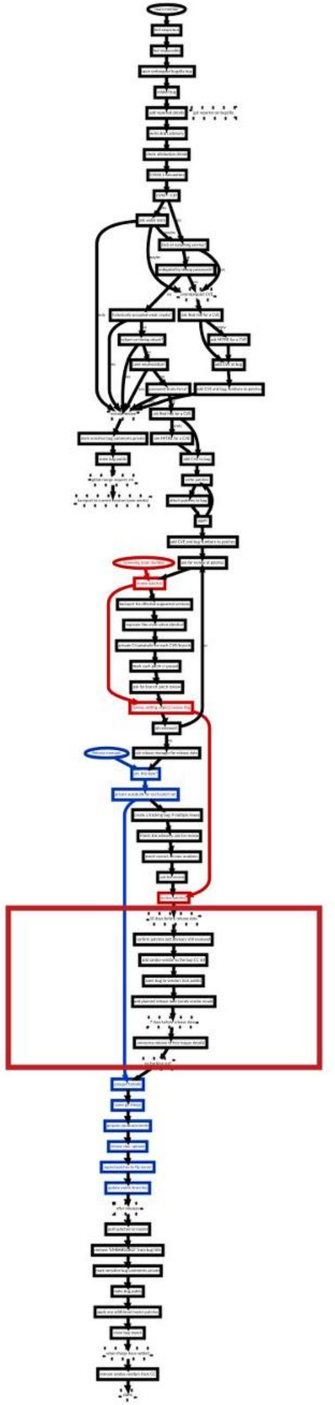
add planned release date (sends vendor email)

7 days before release date

announce release to lists (vague details)

no backing out!

There will be a security release on ..., affecting {AD DC, file services}



10 days before release date

confirm patches and advisory still reviewed

add samba-vendor to the bug CC list

open bug to vendors (not public)

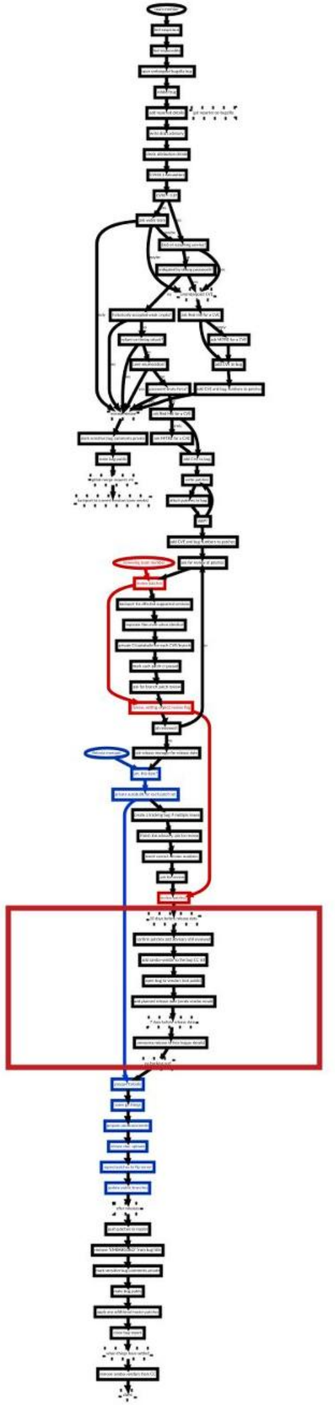
add planned release date (sends vendor email)

7 days before release date

announce release to lists (vague details)

no backing out!

There will be a security release on ..., CVSS X.X affecting AD DC CVSS Y.Y affecting file services



10 days before release date

confirm patches and advisory still reviewed

add samba-vendor to the bug CC list

open bug to vendors (not public)

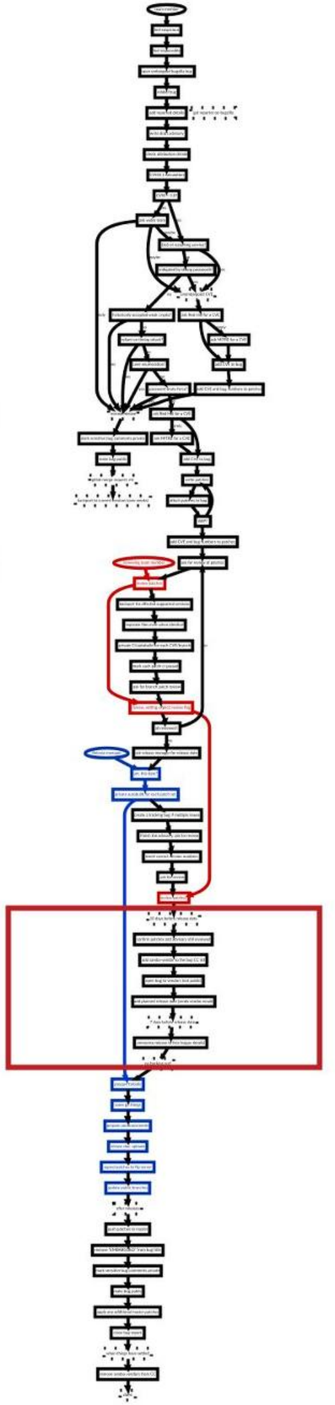
add planned release date (sends vendor email)

7 days before release date

announce release to lists (vague details)

no backing out!

There will be a security release on ..., CVSS X.X affecting AD DC with unusual configuration CVSS Y.Y affecting file services with common configuration



announce release to lists (vague details)

no backing out!

prepare tarballs

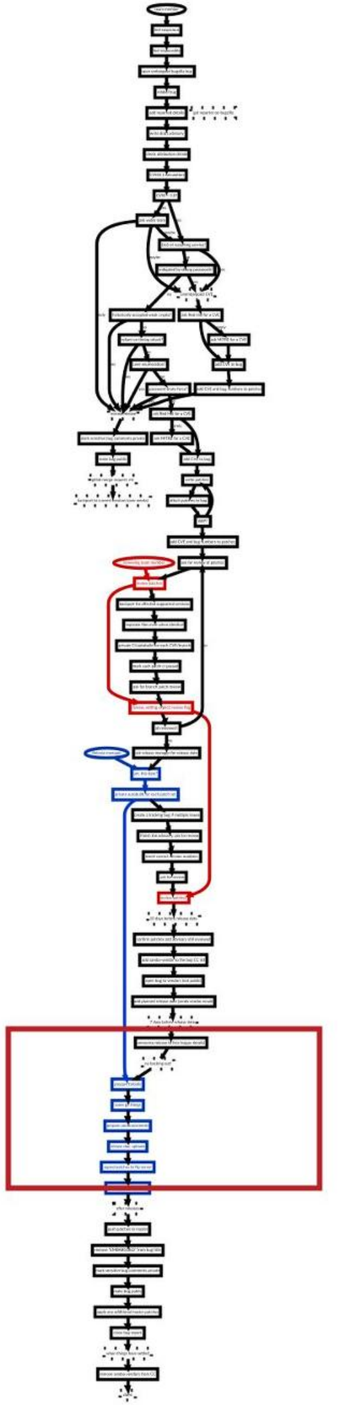
some git things

prepare announcements

release day: uploads

signed patches to ftp server

update public branches



announce release to lists (vague details)

no backing out!

prepare tarballs

some git things

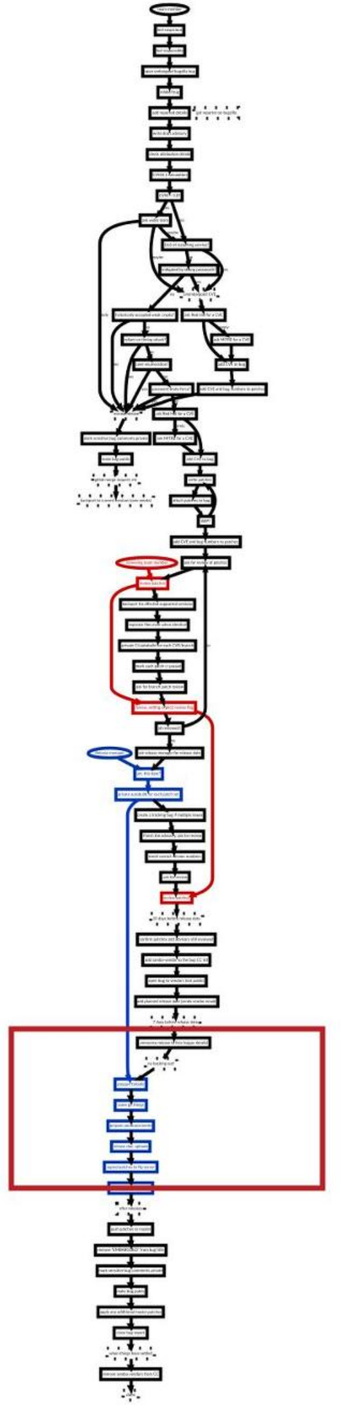
prepare announcements

release day: uploads

signed patches to ftp server

update public branches

but we postpone...



signed patches to ftp server

update public branches

after releases

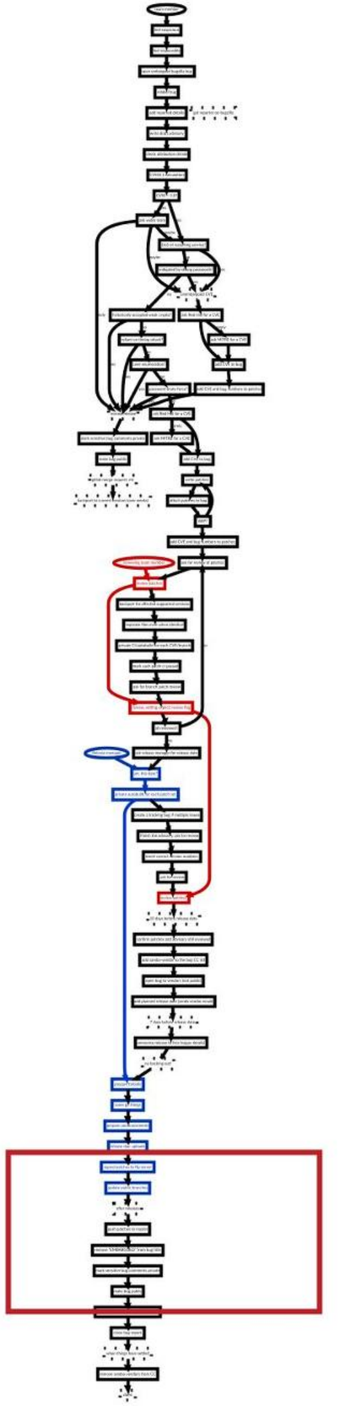
push patches to master

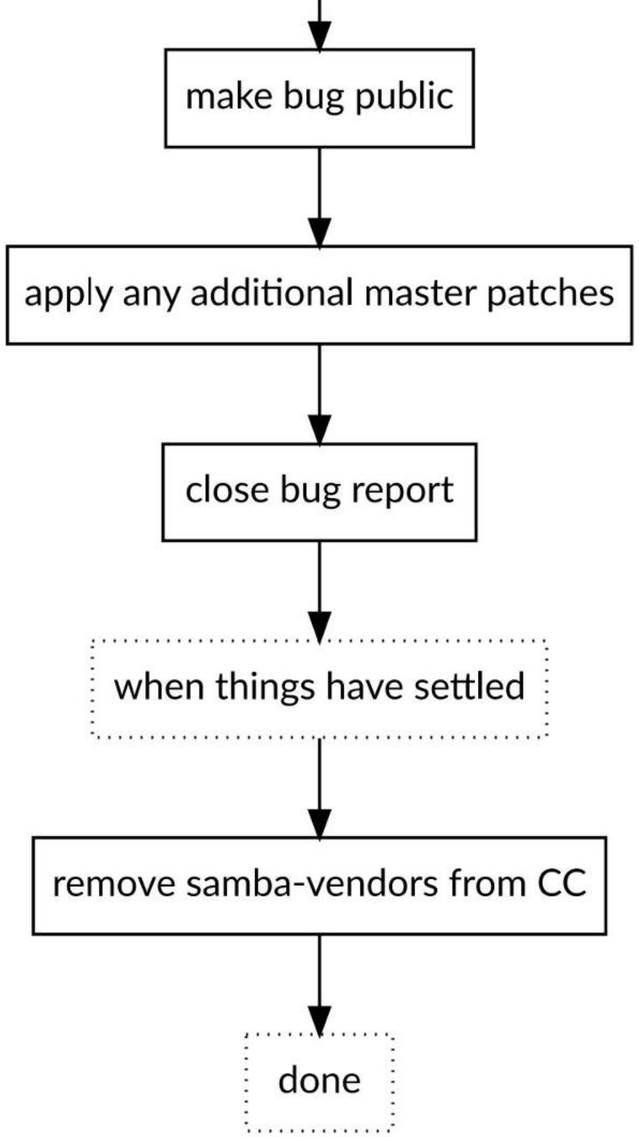
remove “EMBARGOED” from bug title

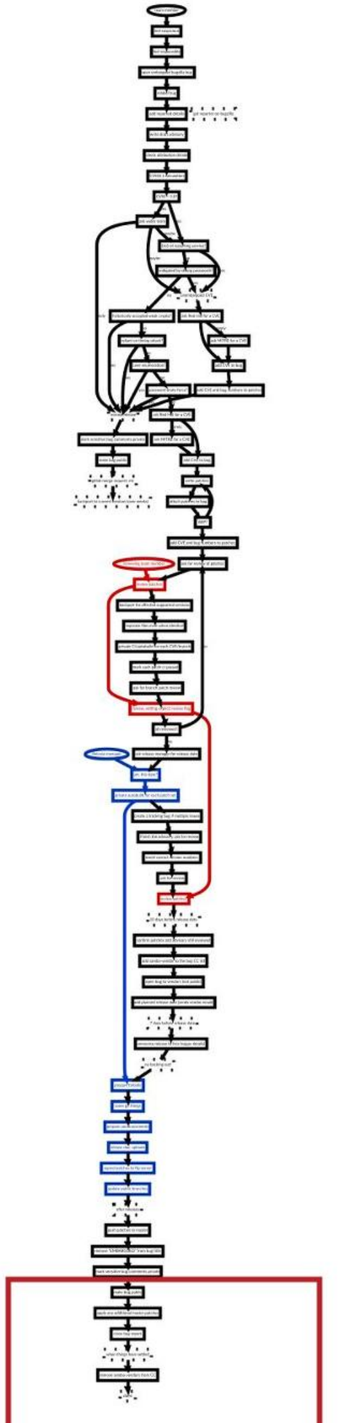
mark sensitive bug comments private

make bug public

apply any additional master patches




make bug public
apply any additional master patches
close bug report
when things have settled
remove samba-vendors from CC
done



Streamlining the process

removing false dependencies

- more checklist than flowchart
- allowing different orders of operation

reduce *n*m* CI requirements

“somebody” to feel responsible for tracking bug

- getting everything is ready before release manager enters.

LLMs makes coordination *more important*

generate exploits from disclosures in minutes

LLMs makes coordination *more important*

generate exploits from disclosures in minutes

maybe this limits the scope for switching to
“normal release with CVE”

If we don't keep up, we can give up

if Samba is not secure, it is not very useful

If we don't keep up, we can give up

if Samba is not secure, it is not very useful

if Samba is *seen* to be insecure, we won't get paid

Trim the bad parts

save time spent fixing bugs in unused code

Trim the bad parts

save time spent fixing bugs in unused code

including unused smb.conf options

Trim the bad parts

save time spent fixing bugs in unused code

including unused smb.conf options

who knows what is unused?

Trim the bad parts

save time spent fixing bugs in unused code

including unused smb.conf options

who knows what is unused?

smb.conf options that have not been mentioned
in the mailing lists this century?

We need money

questions?