

# RVASec 2015

## Vulnerability Coordination and Concurrency

Allen D. Householder

@\_\_adh\_\_

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

© 2015 Carnegie Mellon University



This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0002445

# Vulnerability Coordination and Concurrency



**Introduction & Motivations**

**Survey of Vulnerability Disclosure Models**

**Modeling Coordination as Concurrency**

**What We've Learned (So Far)**

**Conclusion**

# CERT and Vul Disclosure Go Way Back

-----BEGIN PGP SIGNED MESSAGE-----

CA-88:01

CERT Advisory

December 1988

ftpd vulnerability

\*\* The sendma

95:05. \*\*

There have been  
past few weeks.  
the following su

in the  
thered

- 1) Check that you are using version 5.59 of sendmail with the debug option DISABLED. To verify the version try the following commands. Use the telnet program to connect to your mail server. Telnet to your hostname or localhost with 25 following the host. The sendmail program will print a banner which will have the version number in it. You need to be running version 5.59. Version 5.61 will be released on Monday 12/12/1988. Any version less than 5.59 is a security problem.

The following is a sample of the telnet command.

```
% telnet localhost 25
Trying...
```

**SEVERAL  
DAYS  
LATER**

[http://spongebob.wikia.com/wiki/List\\_of\\_time\\_cards](http://spongebob.wikia.com/wiki/List_of_time_cards)

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**       **Edith Ramirez, Chairwoman  
Julie Brill  
Maureen K. Ohlhausen  
Joshua D. Wright  
Terrell McSweeney**

**March 28, 2014**

\_\_\_\_\_ )  
**In the Matter of** )  
 )  
**Fandango, LLC,** )  
**a limited liability company.** )  
\_\_\_\_\_ )

**DOCKET NO. C-4481**

**COMPLAINT**

The Federal Trade Commission, having reason to believe that Fandango, LLC (“respondent”) has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Fandango, LLC (“Fandango”) is a Delaware limited liability company with its principal office or place of business at 12200 W. Olympic Boulevard, Suite 400, Los Angeles, CA 90064.
  
2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

## FANDANGO'S SECURITY FAILURES

15. From March 2009 to March 2013, the Fandango Movies application for iOS failed to validate SSL certificates, overriding the defaults provided by the iOS APIs.
16. Before March 2013, Fandango did not test the Fandango Movies application to ensure that the application was validating SSL certificates and securely transmitting consumers'

**“Fandango does not have a clearly publicized and effective channel for receiving security vulnerability reports, and instead relies upon its general Customer Service system to escalate security vulnerability reports to the proper employees.”**

password reset request and replied with an automated message providing the researcher with instructions on how to reset passwords. Fandango's Customer Service system then marked the security researcher's message as "resolved," and did not escalate it for further review.

18. After Commission staff contacted respondent, Fandango tested the Fandango Movies application for iOS and confirmed that the application failed to validate SSL certificates. Fandango discovered that the vulnerability also affected a separate iOS movie ticketing



[Project Home](#)

[Wiki](#)

**Issues**

[Source](#)

Export to GitHub

New issue

Search

Open issues

for

Search

[Advanced search](#)

## ★ Issue 118: Windows: Elevation of Privilege in ahcache.sys/NtApphelpCacheControl

62 people starred this issue and may be notified of changes.

**Status:** Fixed

**Owner:** [fors...@google.com](#)

**Closed:** Jan 14

**Cc:** [project-...@google.com](#)

**Vendor-**Microsoft

**Product-**Windows-Kernel

**Severity-**High

**Finder-**forshaw

**Reported-**2014-Sep-30

**CCProjectZeroMembers**

**Deadline-**90

**MSRC-**20544

**PublicOn-**2014-Dec-29

**Deadline-**Exceeded

**CVE-**2015-0002

**Fixed-**2015-Jan-13

**Project Member** Reported by [fors...@google.com](#), Sep 30, 2014

**Platform:** Windows 8.1 Update 32/64 bit (No other OS tested)

On Windows 8.1 update the system call NtApphelpCacheControl (the code compatibility data to be cached for quick reuse when new processes are created) cannot add new cached entries as the operation is restricted to admin: AhcVerifyAdminContext.

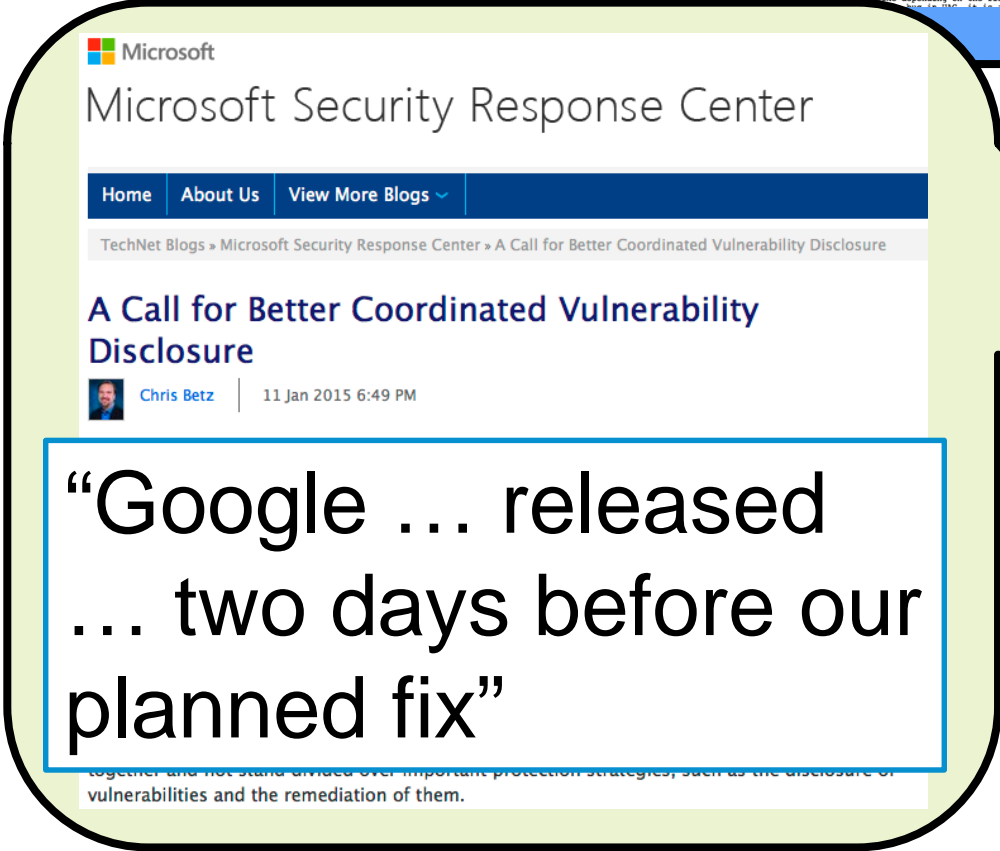
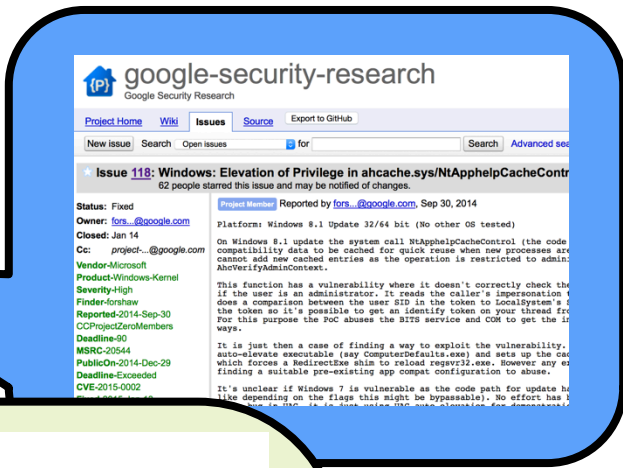
This function has a vulnerability where it doesn't correctly check the caller's impersonation token if the user is an administrator. It reads the caller's impersonation token and does a comparison between the user SID in the token to LocalSystem's SID in the token so it's possible to get an identify token on your thread from LocalSystem. For this purpose the PoC abuses the BITS service and COM to get the identify token in various ways.

It is just then a case of finding a way to exploit the vulnerability. The PoC uses a process to auto-elevate executable (say ComputerDefaults.exe) and sets up the cache configuration which forces a RedirectExe shim to reload regsvr32.exe. However any exploit would be finding a suitable pre-existing app compat configuration to abuse.

It's unclear if Windows 7 is vulnerable as the code path for update has changed (and is like depending on the flags this might be bypassable). No effort has been made to find a bug in UAC, it is just using UAC auto-elevation for demonstration purposes.



# Google

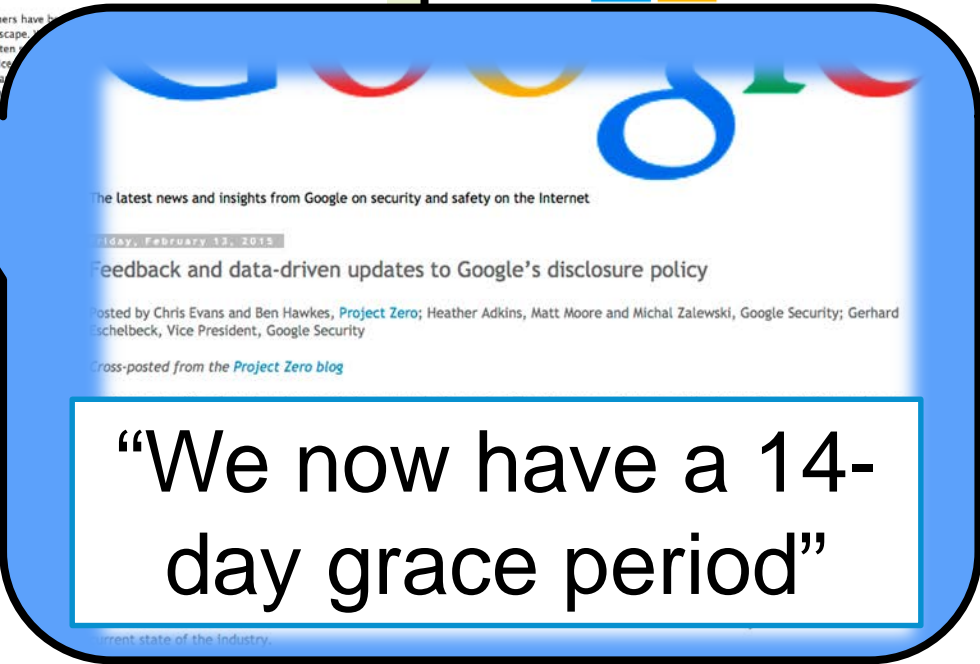
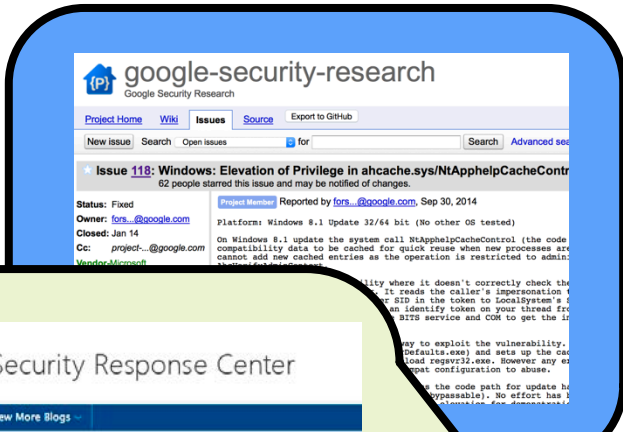


“Google ... released ... two days before our planned fix”



# Microsoft

# Google



# Motivations

Resurgent disclosure kerfuffles

Proliferation of novice vendors

- There are more new vendors than there is vulnerability coordination experience to go around
- Networked services bolted onto existing products
  - cars, refrigerators, door locks, light bulbs, medical devices, industrial control systems
- Anyone can become an app creator

# Motivations

## Vul markets & bug bounties change the flow of information

See also Katie Moussouris @ OWASP AppSec 2015 <https://youtu.be/IPTYyg0OzYQ>

## Third party libraries are more important than ever

- Yet library vuls are significantly harder to coordinate well

See also Kymberlee Price & Jake Kouns @ DerbyCon 4 <https://youtu.be/sLxcOtEfGvg>

## Rampant growth in both awareness of security and the security industry itself

- Vul disclosure discussions are older than today's participants
  - “Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done.” – A.C. Hobbs, 1853 (HT: Matt Blaze, Steve Bellovin)

– <http://www.crypto.com/hobbs.html>

# Motivations

“We now have multiparty, multifaceted coordination needs. These are cross-industry requirements, which means we need to now consider phasing our disclosures. This requires us to open the genie box and **reconsider our approach in a more organized manner**. No longer can a researcher jump out and save the Internet from itself, since its complexity is beyond that stage. A researcher may understand the bug, but **the system of systems and the interactions require a broader group effort** .”

- Peter Allor, Federal Security Strategist, IBM Security

<http://securityintelligence.com/determining-the-responsibility-of-a-vulnerability-disclosure/>

# Motivations

“We now have multiparty, multifaceted coordination needs. These are cross-industry requirements, which means we need to now consider phasing our disclosures. This requires us to open the genie box and **reconsider our approach in a more organized manner**. No longer can a researcher jump out and save the Internet from itself, since its complexity is beyond that stage. A researcher may understand the bug, but **the system of systems and the interactions require a broader group effort** .”

- Peter Allor, Federal Security Strategist, IBM Security

<http://securityintelligence.com/determining-the-responsibility-of-a-vulnerability-disclosure/>

# Modeling the Process



# Why Create Models?

Models enable conversations about the process

- without devolving into arguments over the specifics of individual disclosures.

Models can be subjected to analysis

- and are easier to change than day-to-day operations.

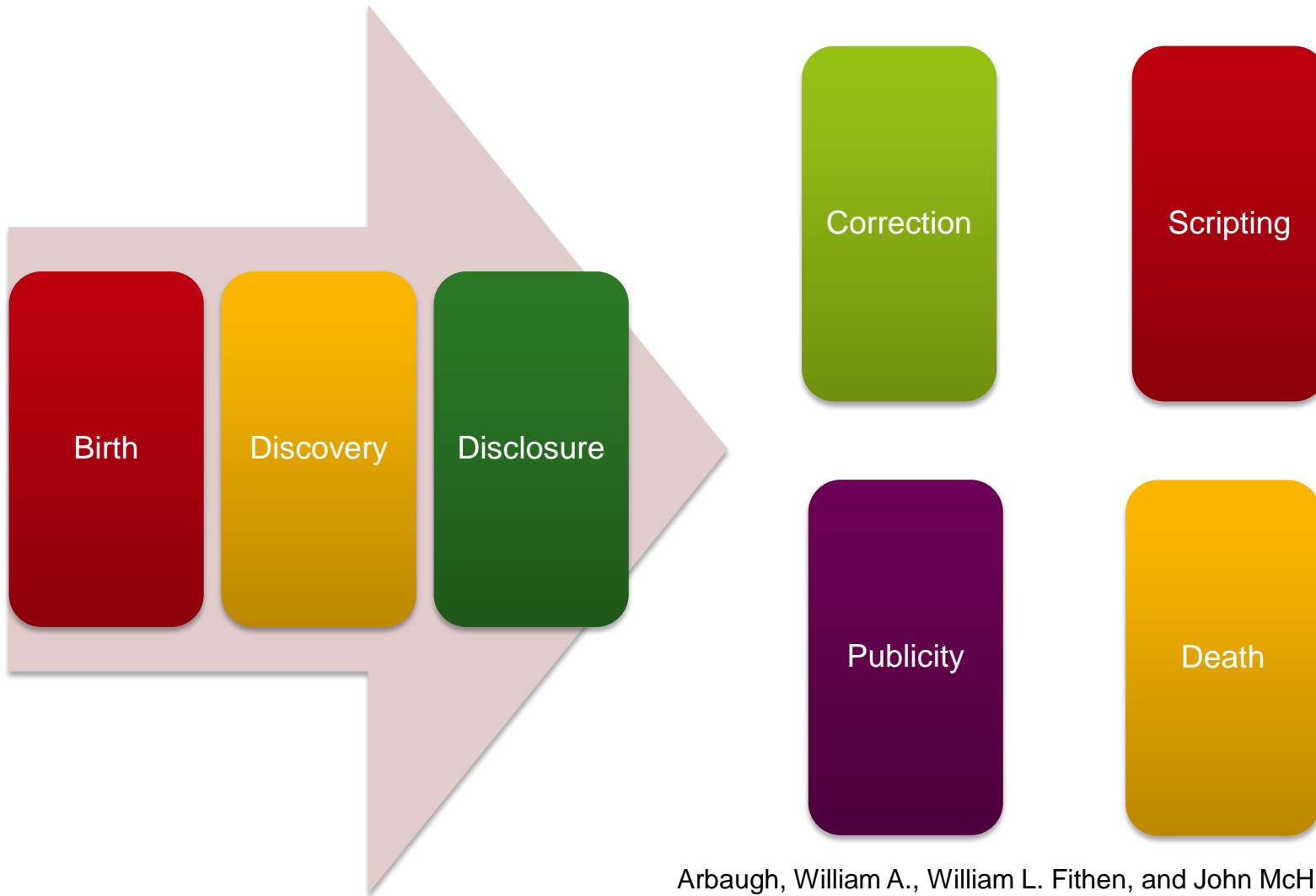
Models promote learning and knowledge transfer

- by removing unneeded detail

Reasoned disagreement about a model leads to better models.

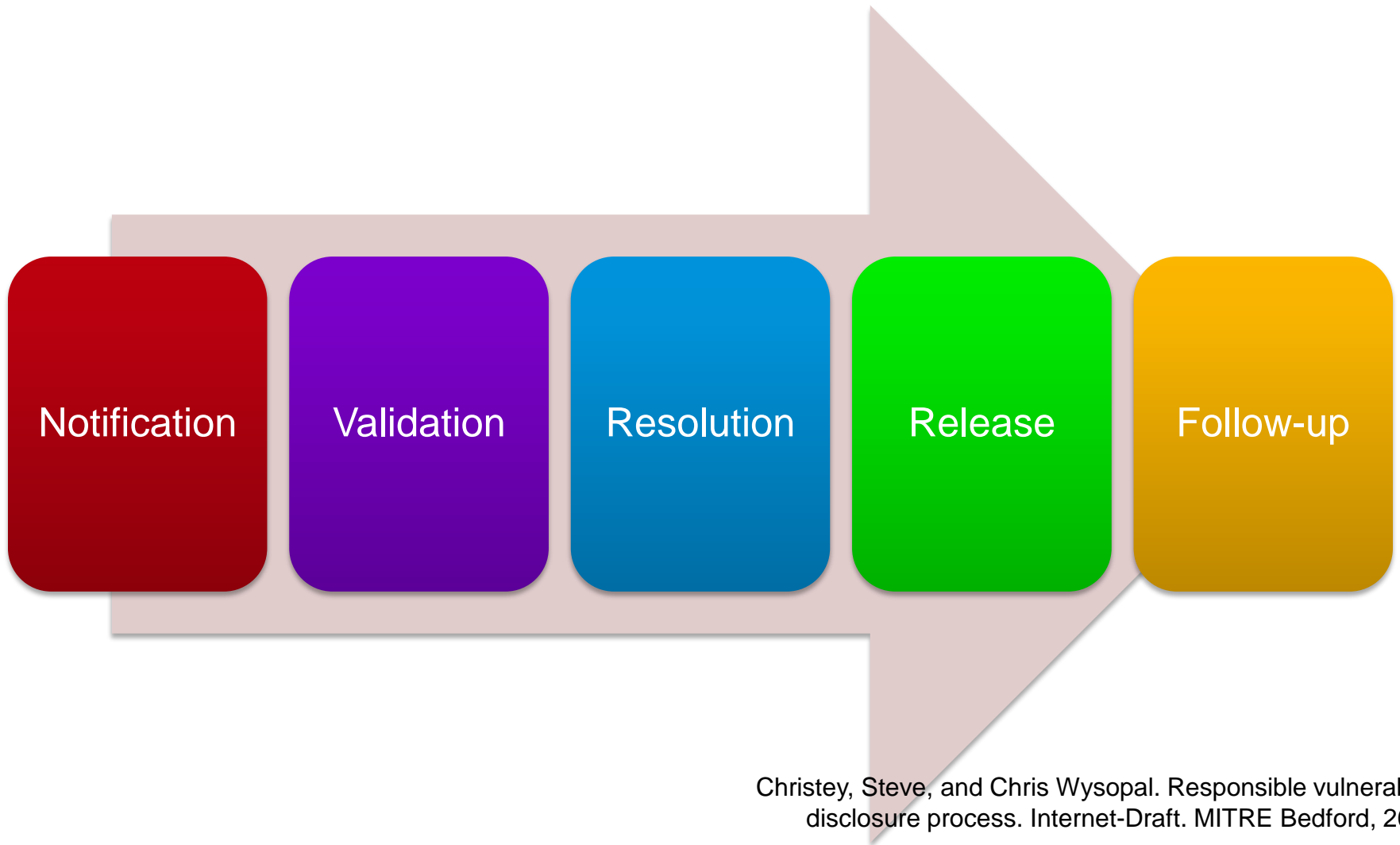


# Arbaugh, Fithen, McHugh (2000)



Arbaugh, William A., William L. Fithen, and John McHugh. "Windows of vulnerability: A case study analysis." *Computer* 33.12 (2000): 52-59.

# Christey, Wysopal (2002)



Christey, Steve, and Chris Wysopal. Responsible vulnerability disclosure process. Internet-Draft. MITRE Bedford, 2002.

[draft-christey-wysopal-vuln-disclosure-00.txt](#)

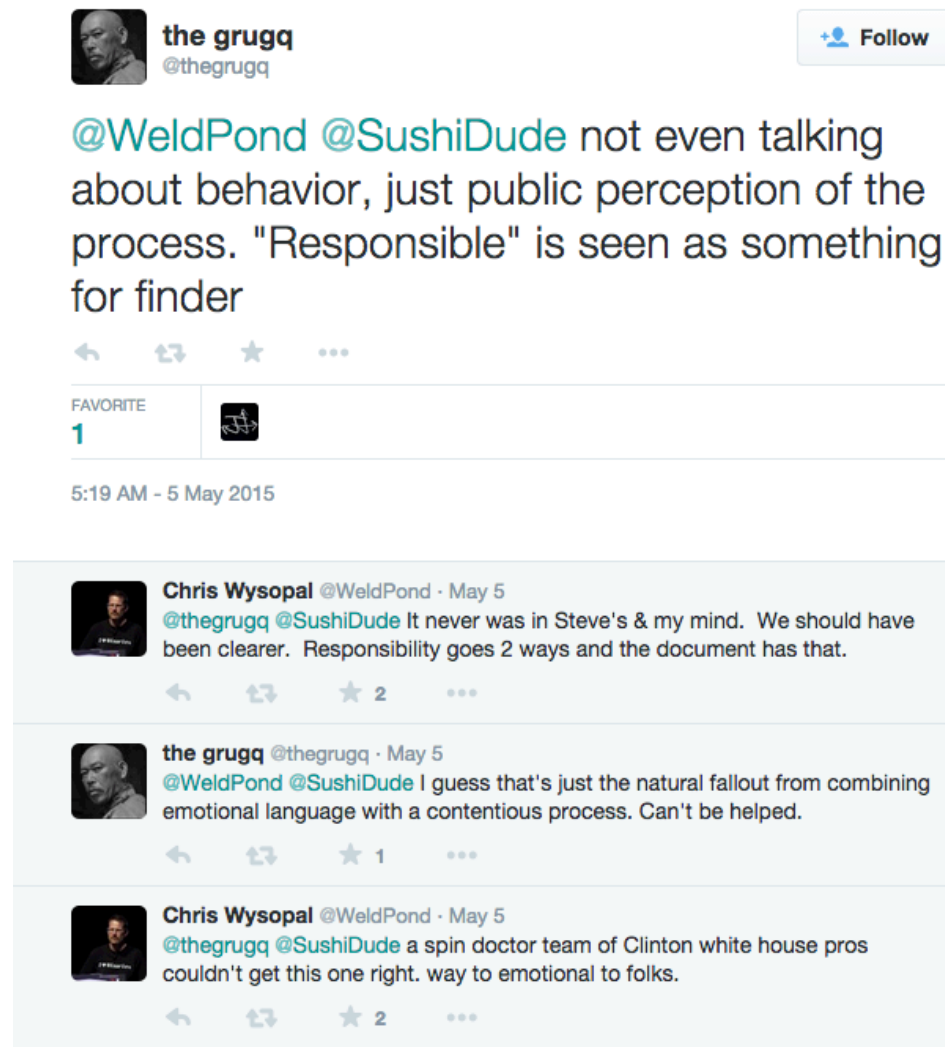
# “Responsible” Disclosure?


*Responsible* implies a value judgment

...which turns it into an argument over competing perspectives

*Coordinated Disclosure* is our preferred term

...but that doesn't always mean wait for the vendor to release a patch





“You're going to find that many of the truths we cling to depend greatly on our own point of view”

# NIAC Vulnerability Disclosure Framework (2004)

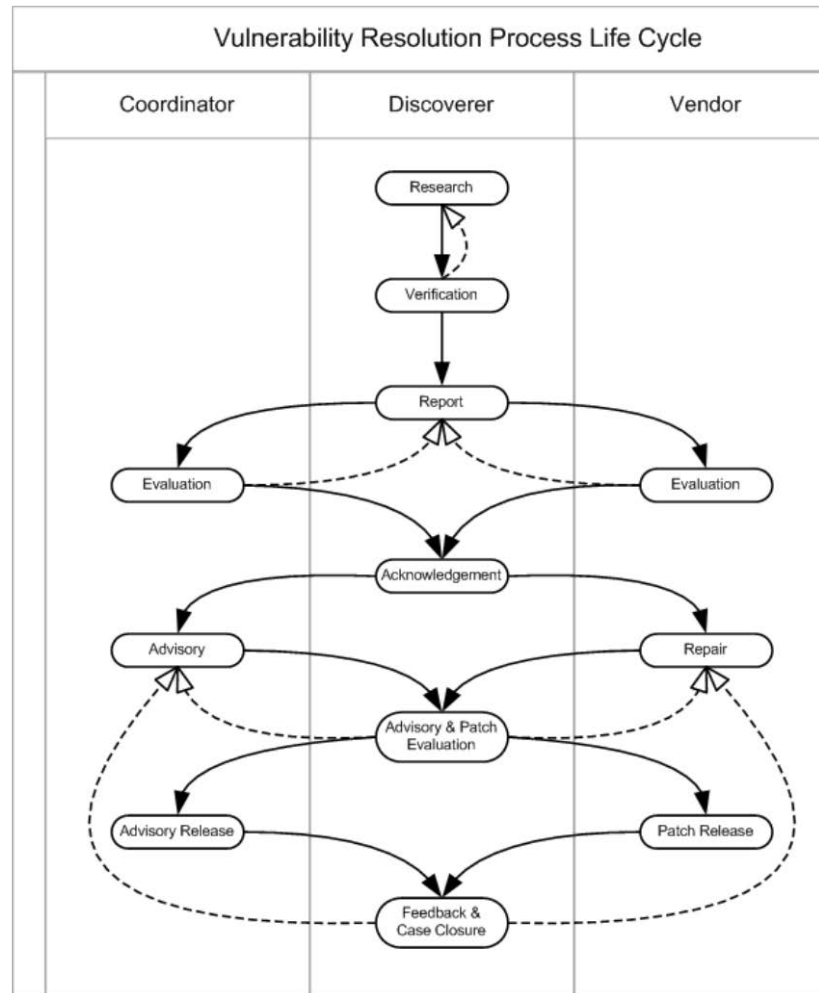


Figure 1: Vulnerability Resolution Process Life Cycle

<https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf>

Chambers, et al.

# OIS Guidelines for Security Vulnerability Reporting and Response (2004)

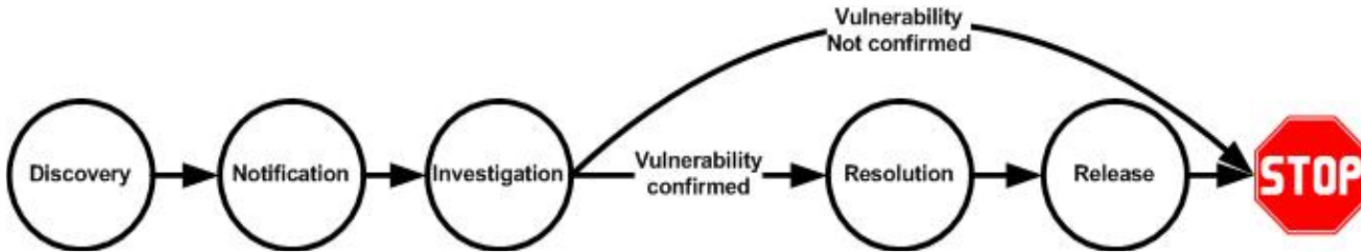


Figure 1. Basic Steps in the Security Vulnerability Reporting and Response Process

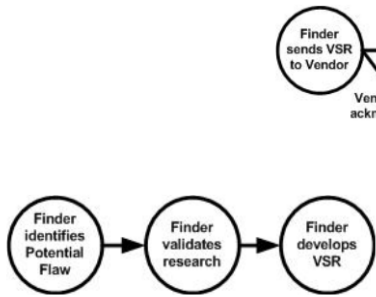


Figure 2. Steps in Discovery Phase

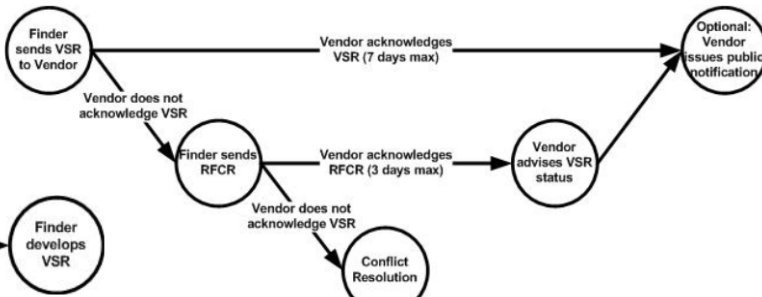


Figure 3. Steps in Notification Phase

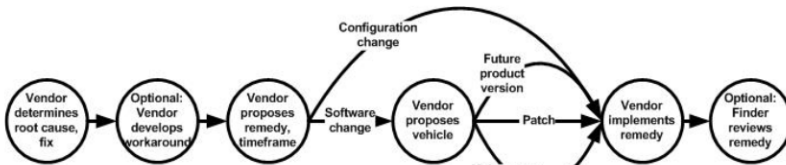


Figure 5. Steps in Resolution Phase

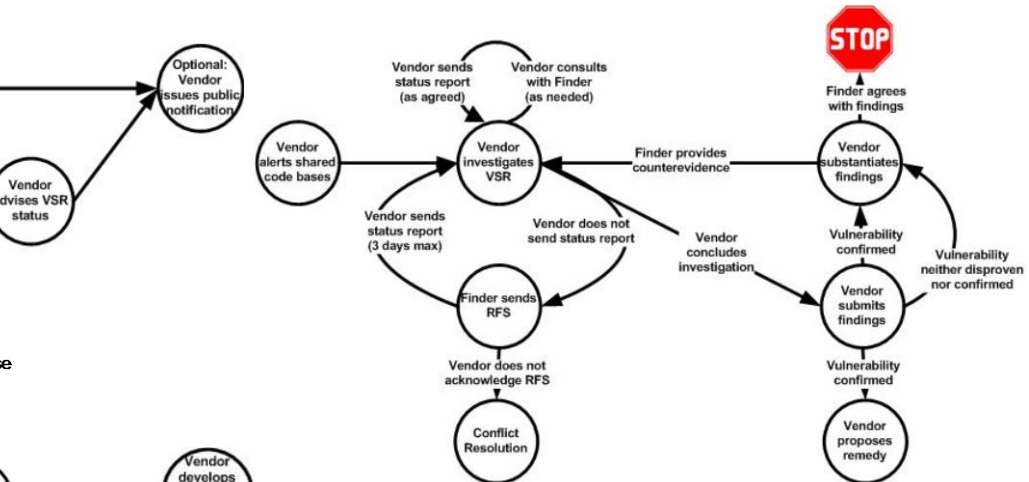


Figure 4. Steps in Investigation Phase

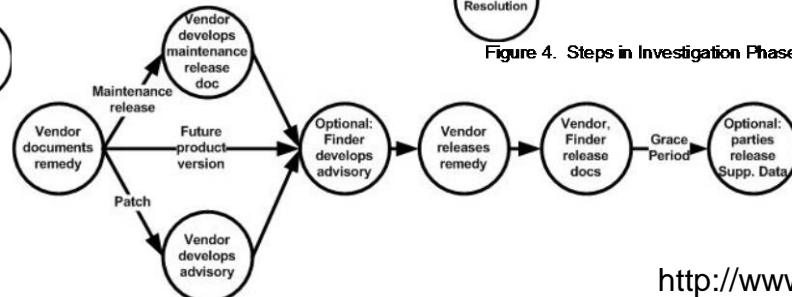
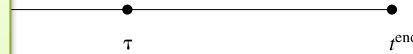


Figure 6. Steps in Release Phase

<http://www.oisafety.org/>

# Arora, Telang, and Xu (2008)

“as long as the vendor does not internalize the entire user loss, the vendor will release the patch later than is socially optimal, unless threatened with disclosure.”



4 Social Cost as a Function of  $T$

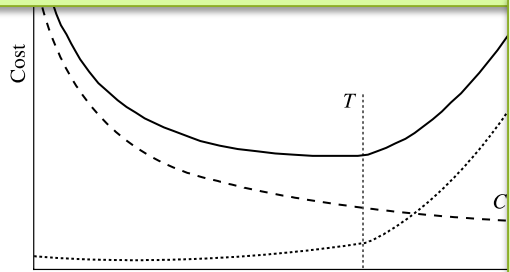


Figure 3 Patch Development Time  $\tau$  as a Function of Period  $T$

“The more responsive the vendor is to user losses, the more aggressive the social planner can be by setting a shorter protected period.”

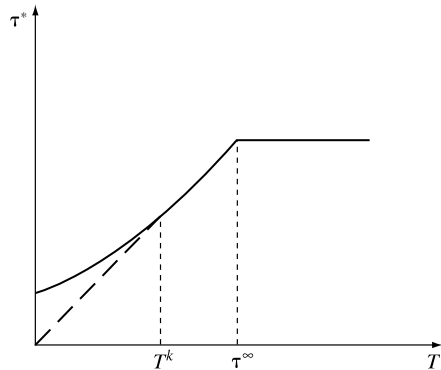
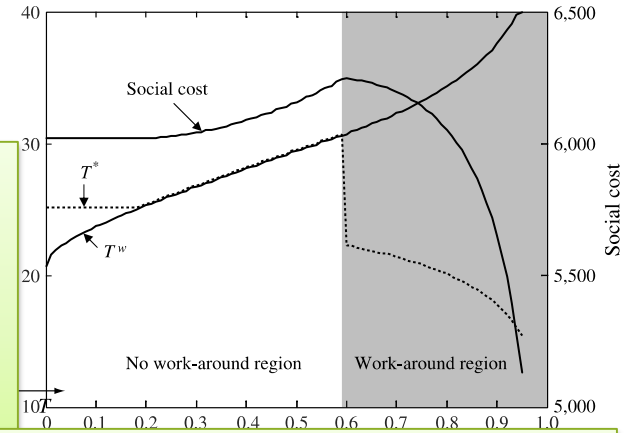


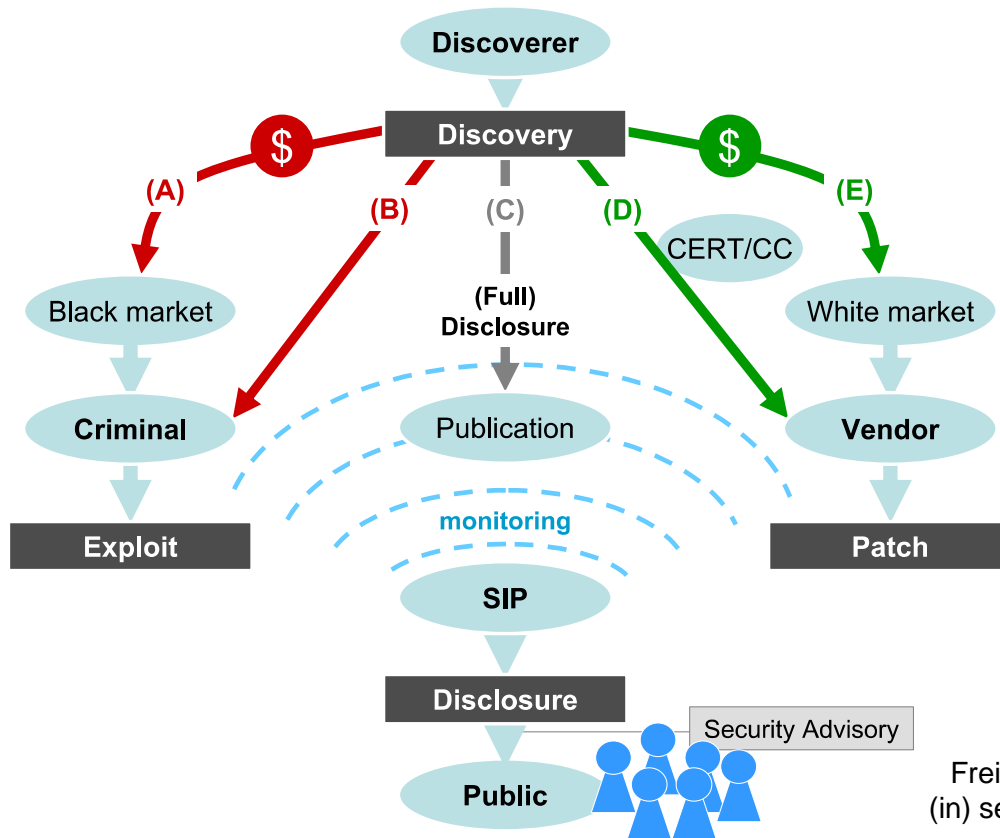
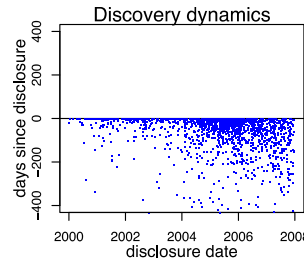
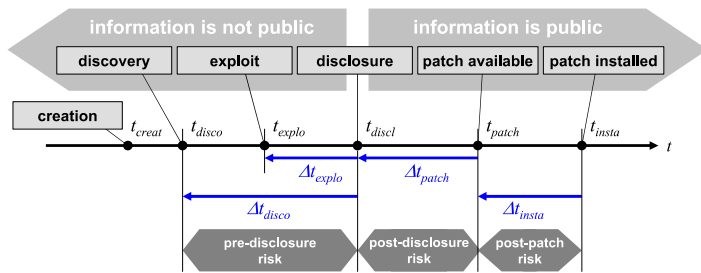
Figure 9 Social Cost,  $T^*$  and  $T^w$  as a Function of Smart Users



“In general, both an instant disclosure and a secrecy policy are suboptimal, although numerical simulations suggest that instant disclosure is particularly inefficient.”

Arora, Telang, and Xu: Optimal Policy for Software Vulnerability Disclosure Management Science 54(4), pp. 642–656, © 2008 INFORMS

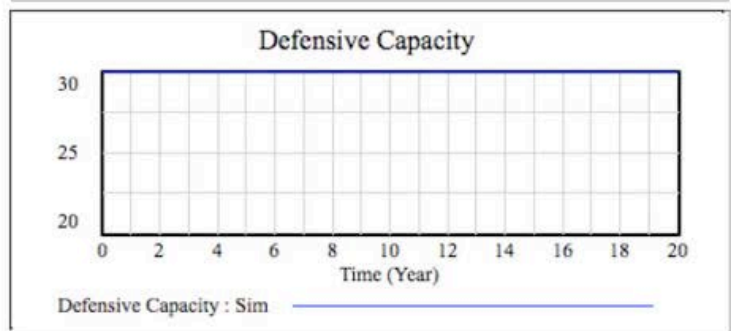
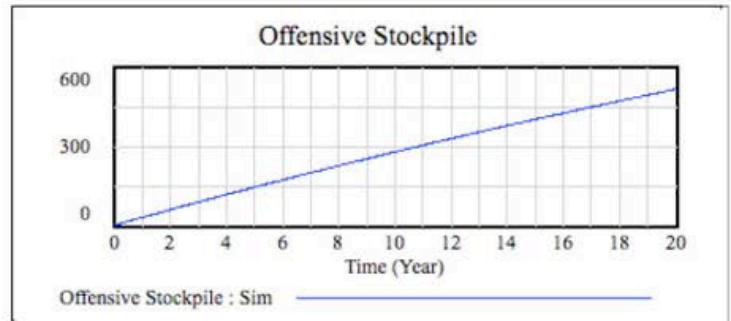
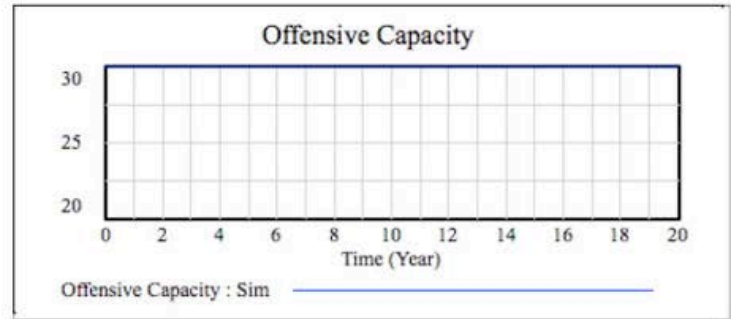
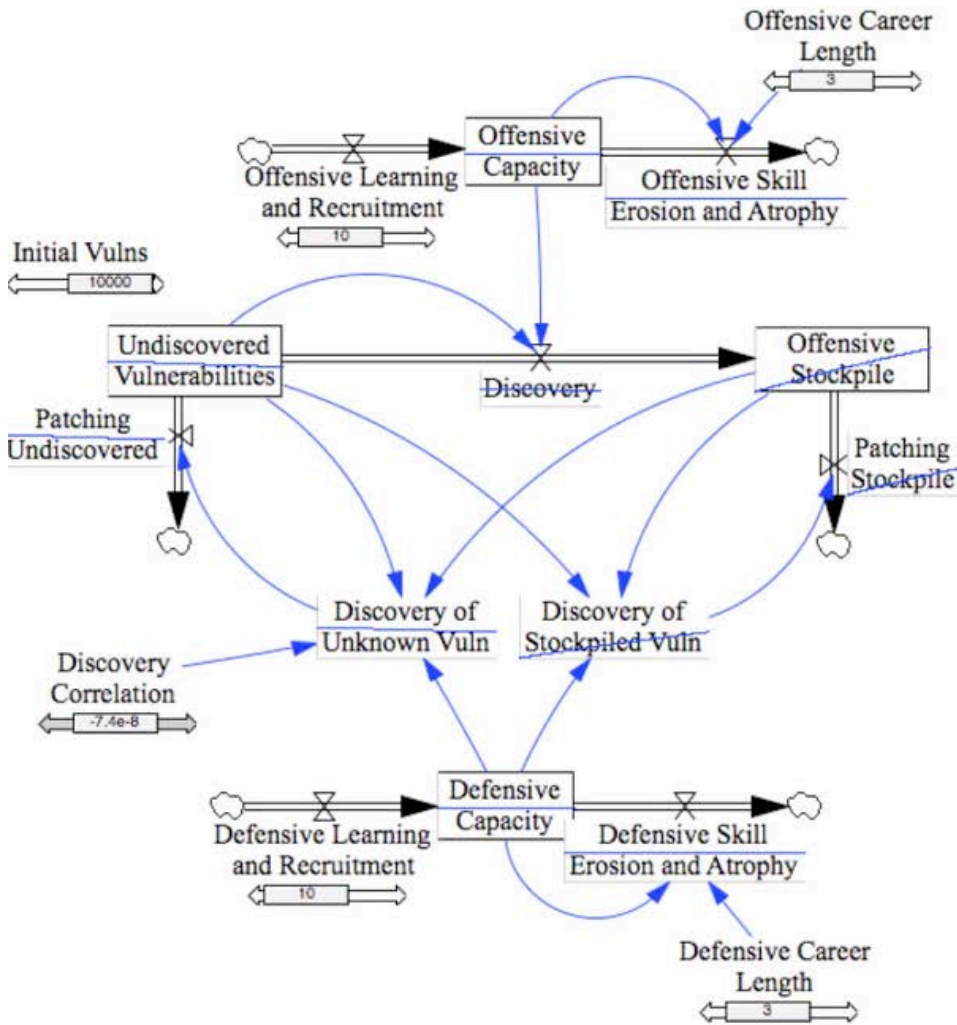
# Frei, Shatzmann, Plattner, & Trammell (2009)



Frei, Stefan, et al. "Modeling the security ecosystem-the dynamics of (in) security." *Economics of Information Security and Privacy*. Springer US, 2010. 79-106.



# The Wolves of Vuln Street (2015)



<https://hackerone.com/news/the-wolves-of-vuln-street>

Moussouris, Siegel, Houghton, & Ellis

# What's missing from prior models?

Early models were primarily narrative, prescriptive advice

- Many imply more synchronization than we observe in the wild
- “We rarely encounter cases with CERT/CC’s preferred ordering” - Arbaugh, et al. (2000)

Later models start to incorporate

- social cost
- participant motives
- money and markets

But they don't illuminate how and why coordinated vulnerability disclosure can fail

Modeling the Process  
**Concurrency**



# Why Create a Concurrency Model?

Vulnerability disclosure is a multiparty, human-centric, concurrent process

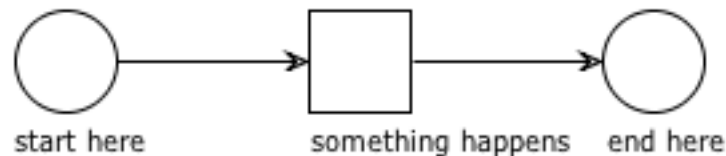
- Vendors
- Researchers
- Coordinators
- Other stakeholders
  - Service providers
  - Governments
  - Users

Each party represents a complex interaction of many people, processes, policies, and procedures

# Intro to Petri Nets

Used to model distributed processes as a network of nodes and arcs.

Nodes can be either *places* (circles), or *transitions* (boxes).



*Arcs* (arrows) connect places to transitions and vice versa.

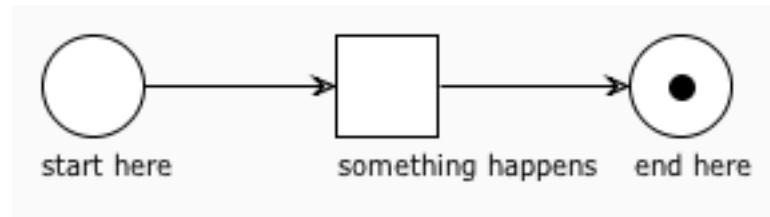
- Places can't connect to places
- Transitions can't connect to transitions

All Petri Net diagrams in this presentation were created using WoPeD

<http://www.woped.org/>

# Intro to Petri Nets

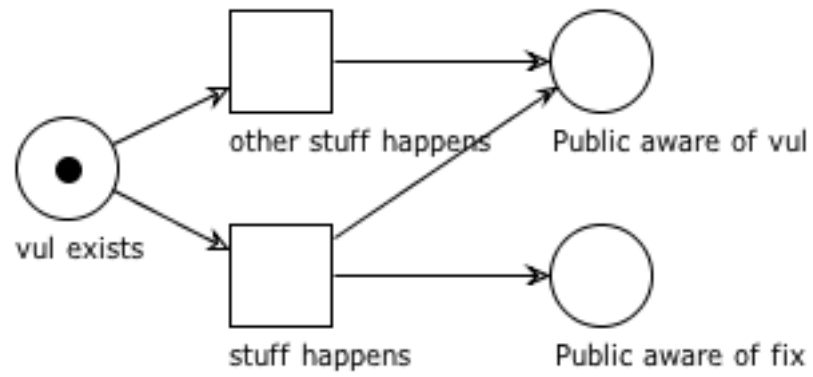
Places can hold *tokens*, which mark the state of a process.



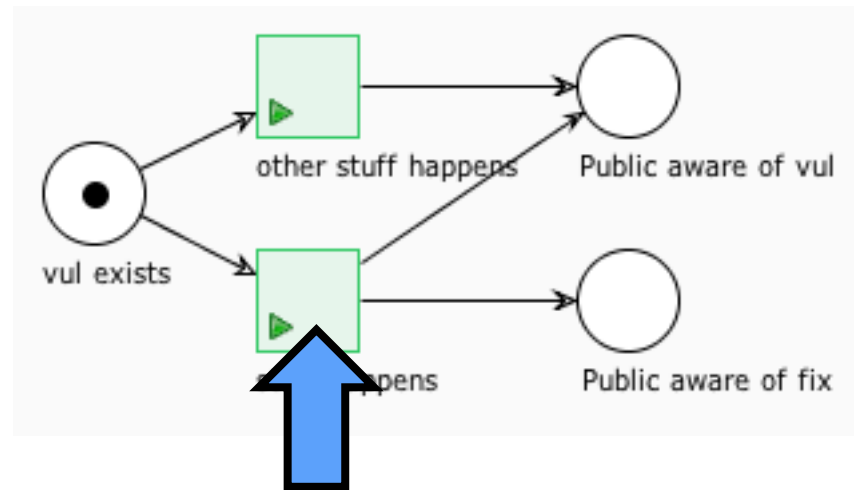
Transitions represent events that change the state of the process.

- A transition can *fire* when all the places immediately upstream of it are occupied by tokens (i.e., when it is *enabled*).
- When a transition fires, it consumes tokens from its inputs and places tokens in its outputs.

# A Simple Model

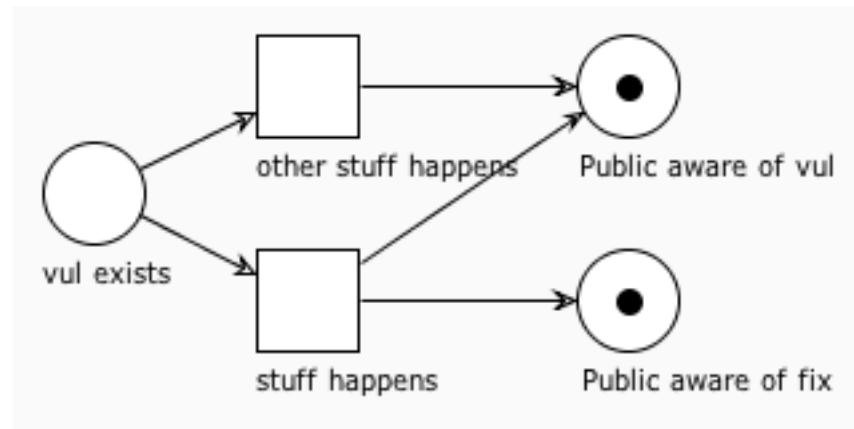


# A Simple Model

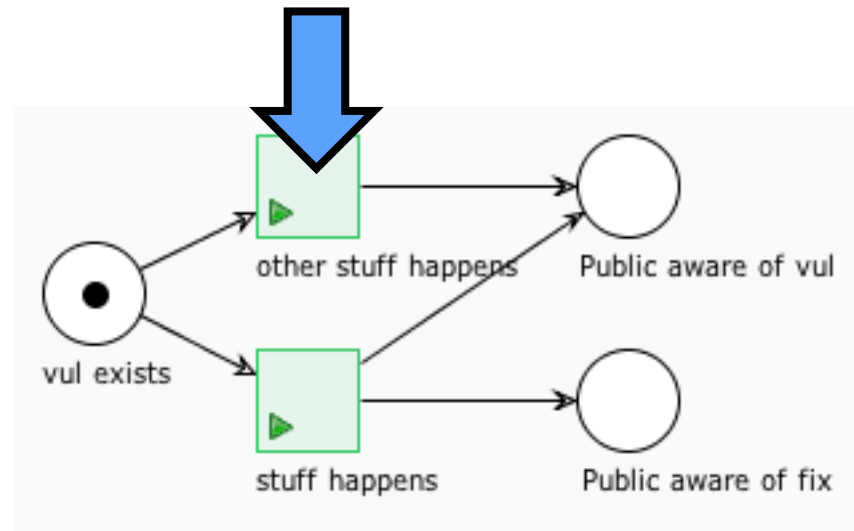




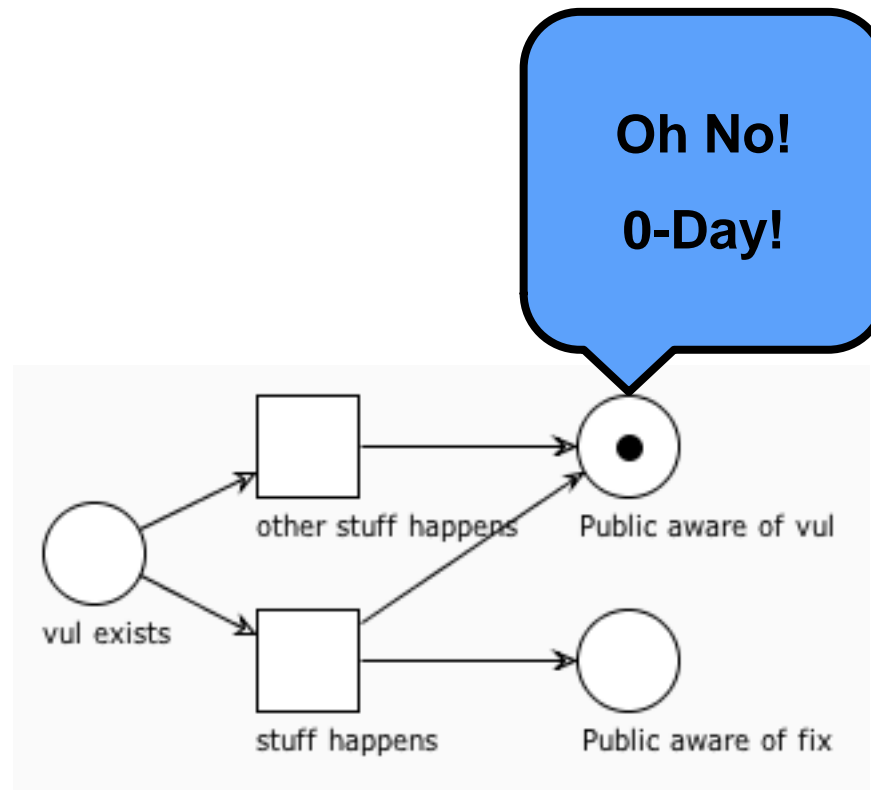
# A Simple Model



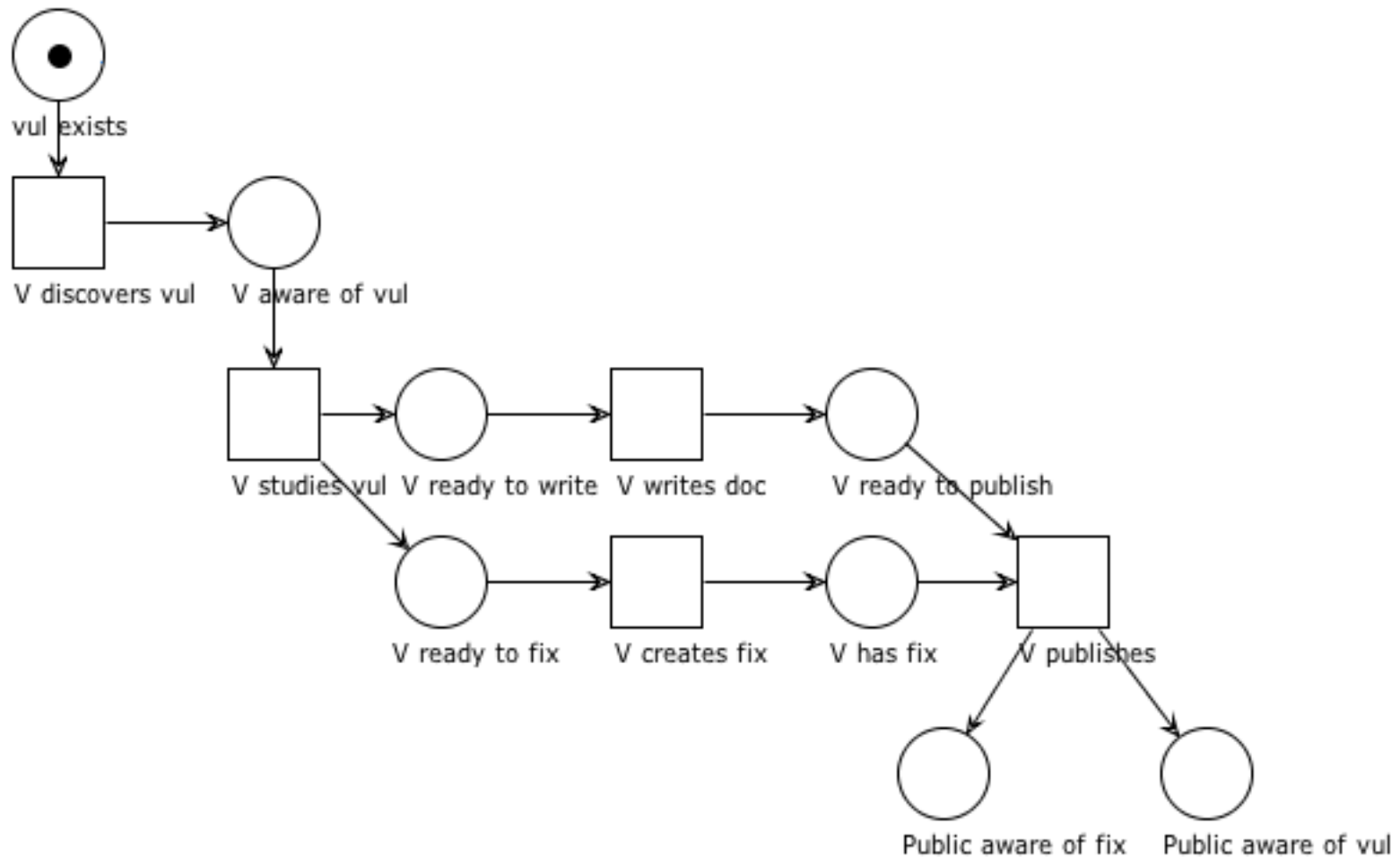
# A Simple Model



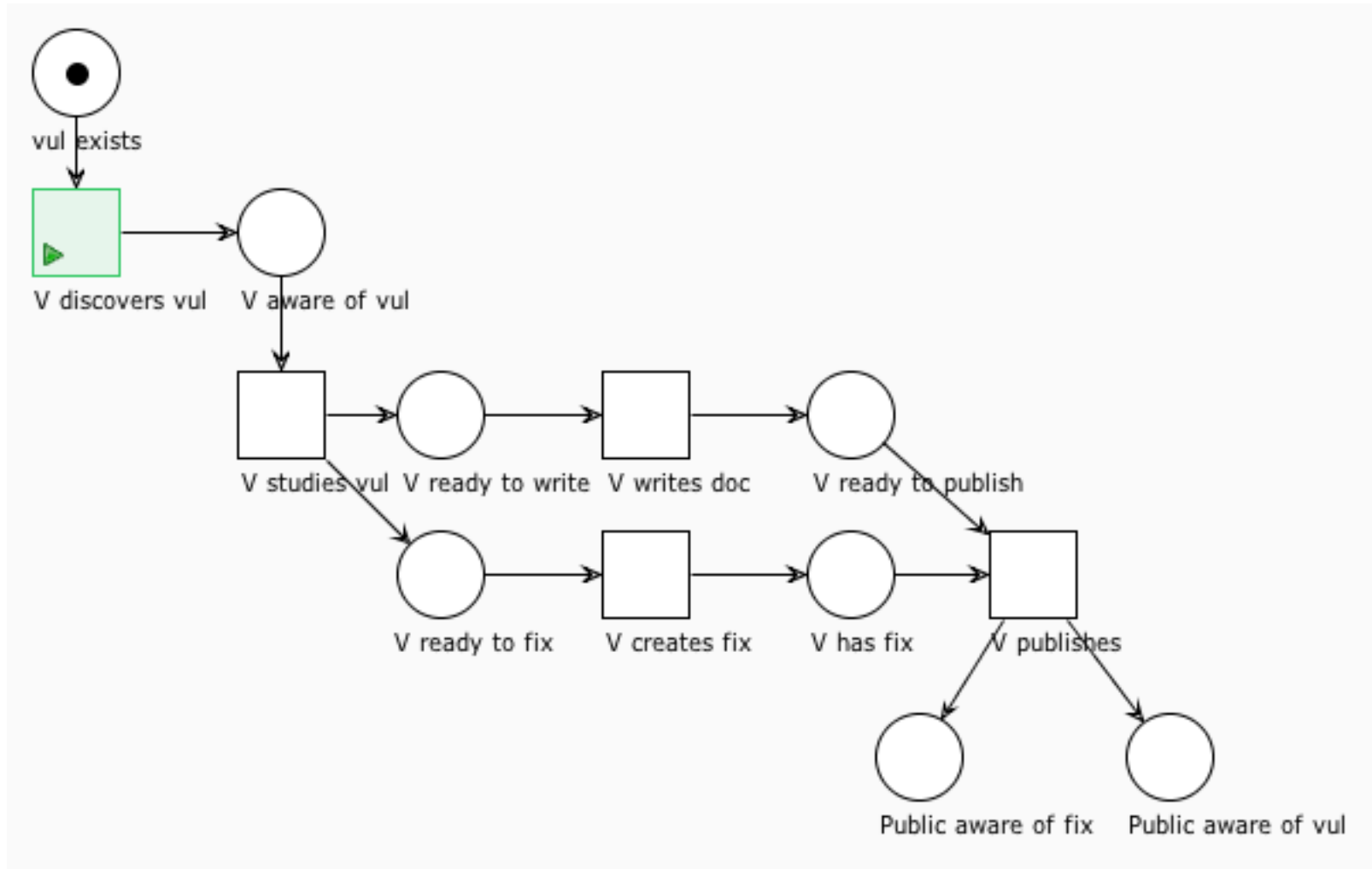
# A Simple Model



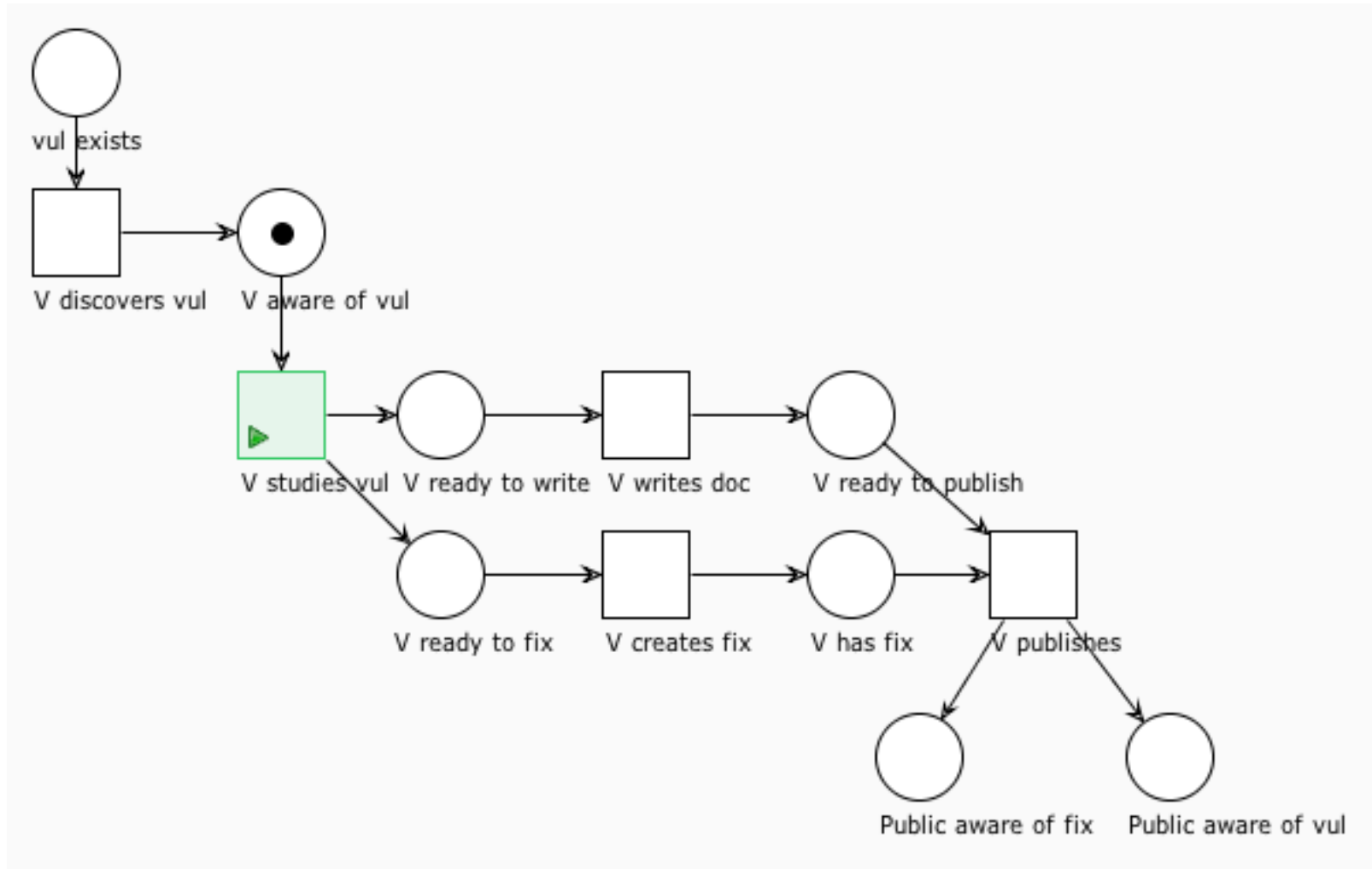
# Vendor Model



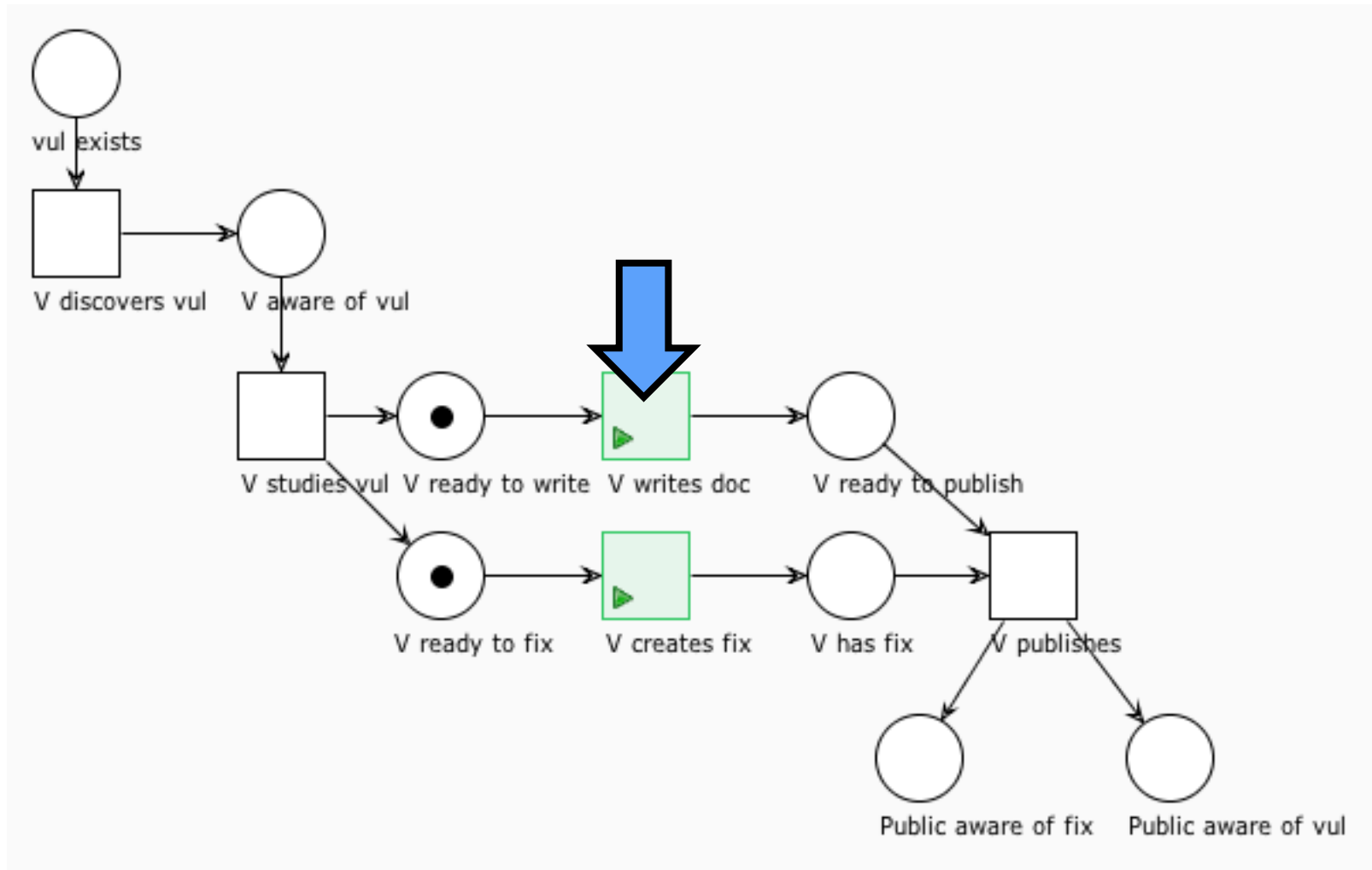
# Vendor Model



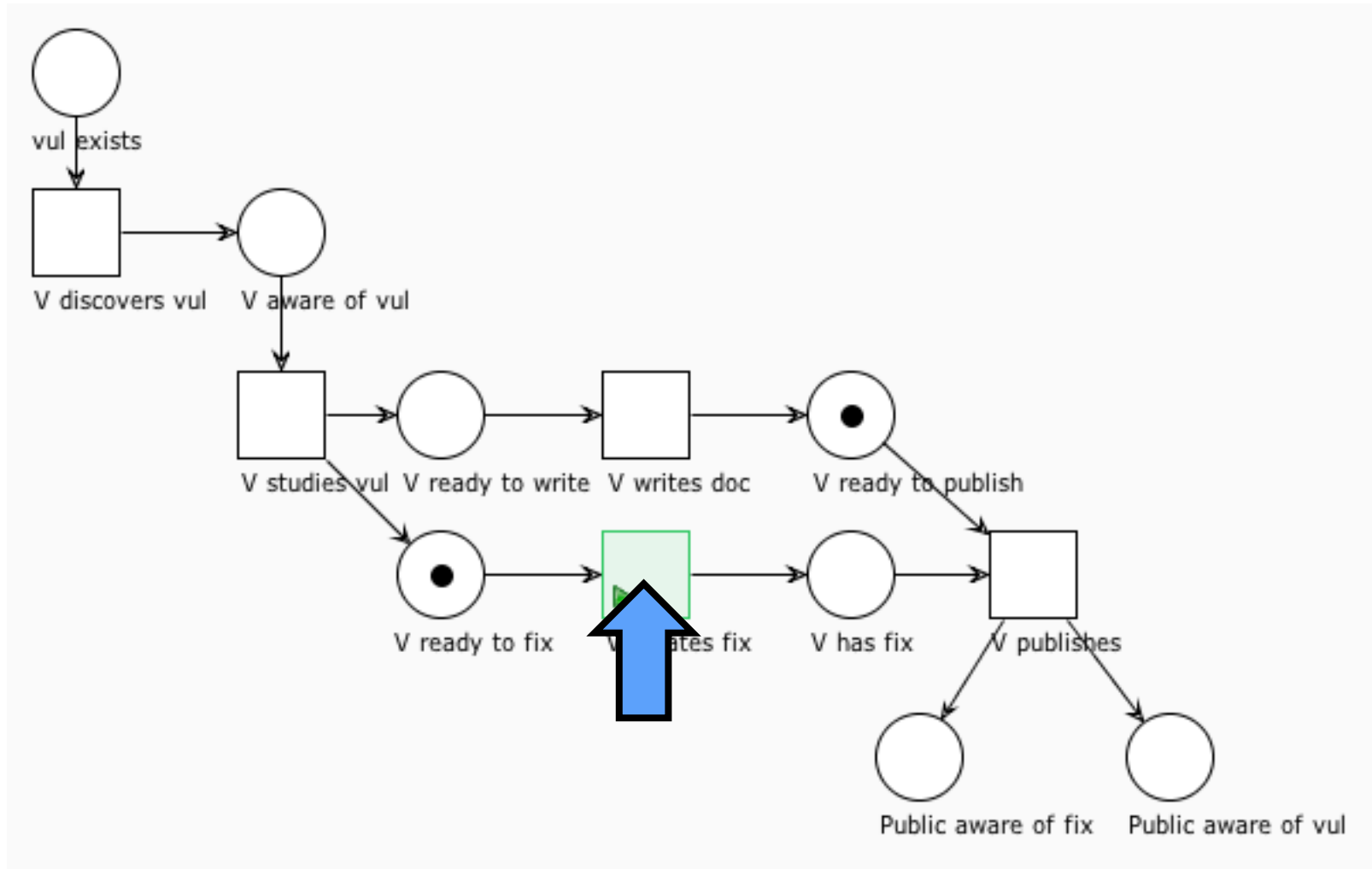
# Vendor Model



# Vendor Model

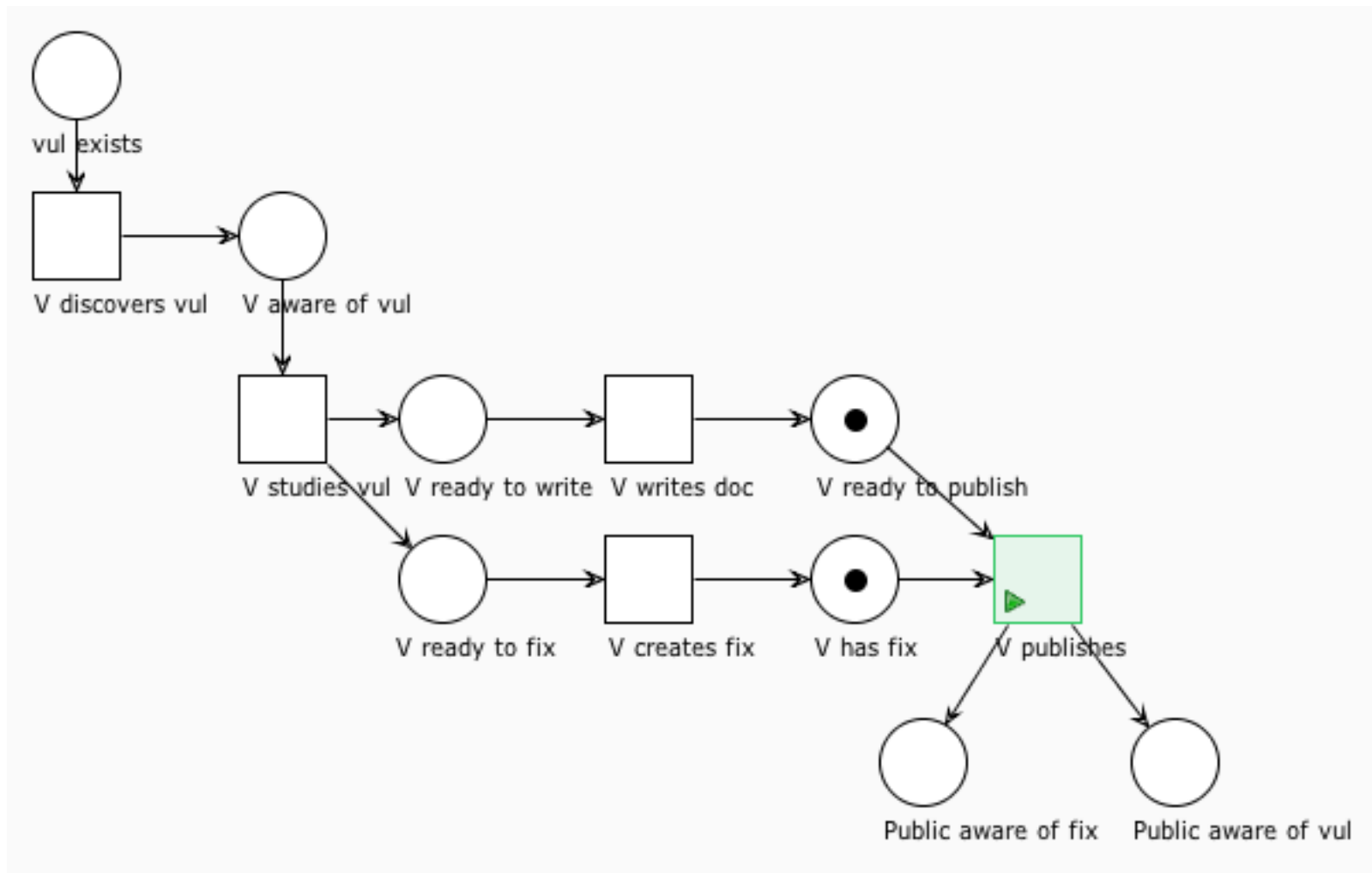


# Vendor Model

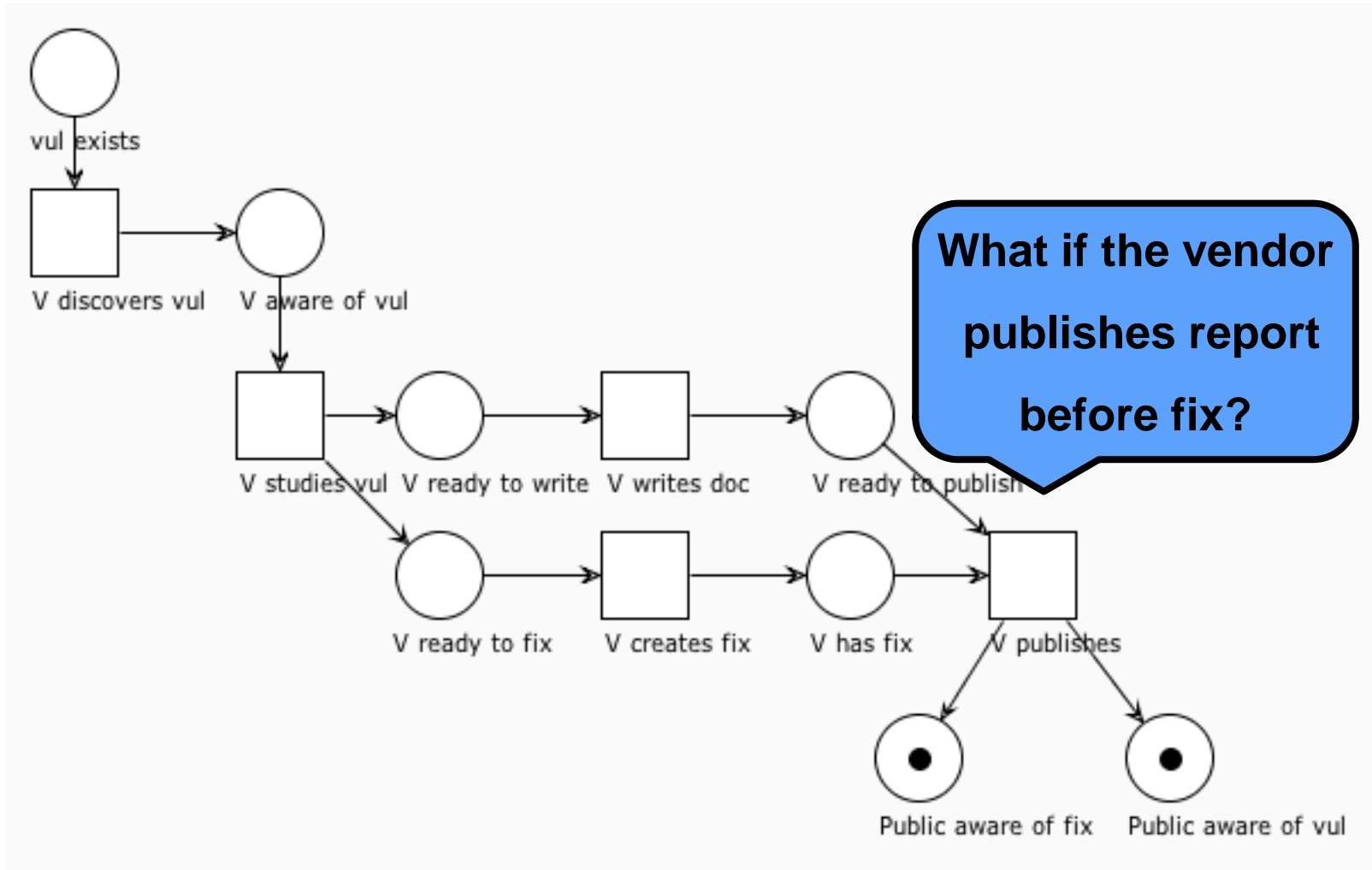




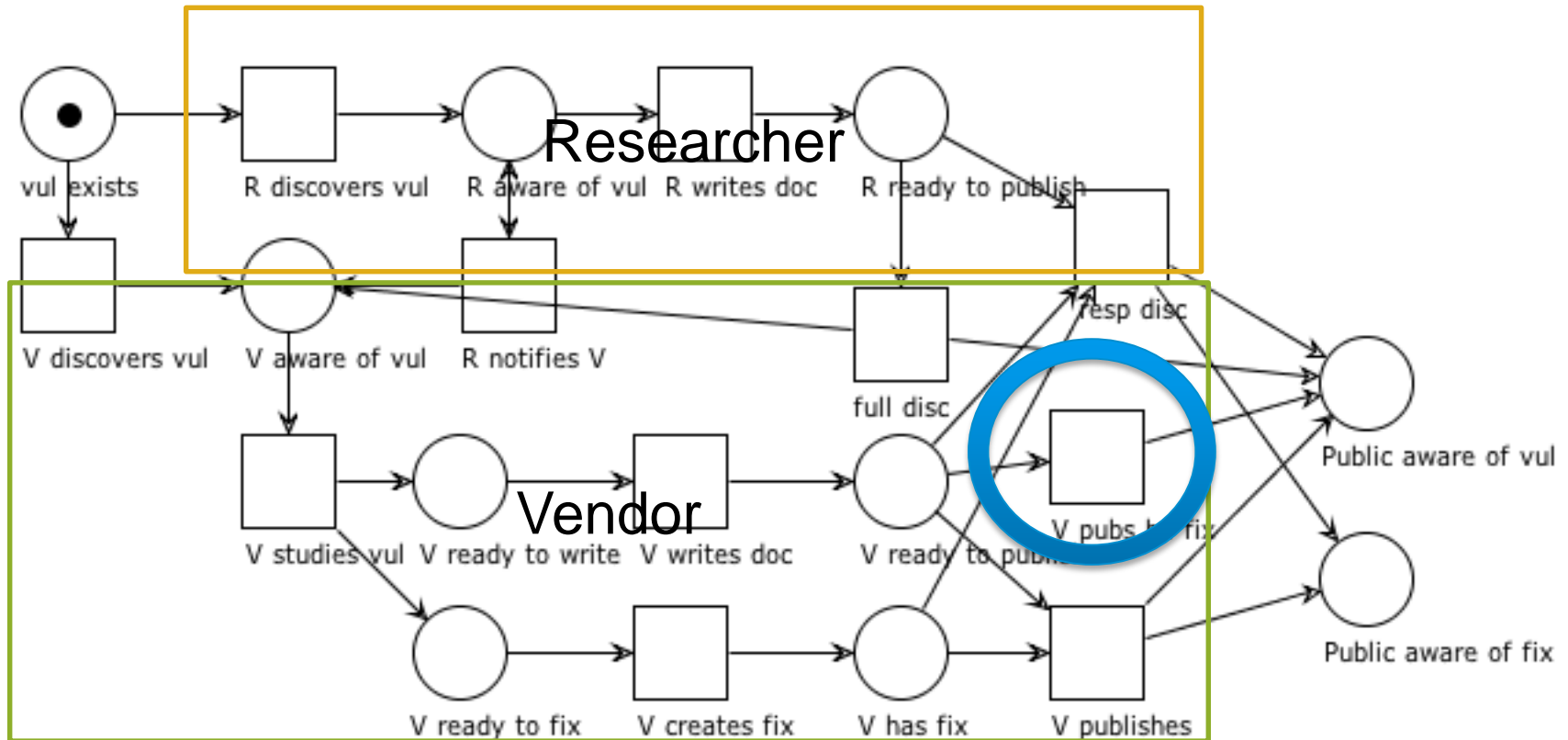
# Vendor Model



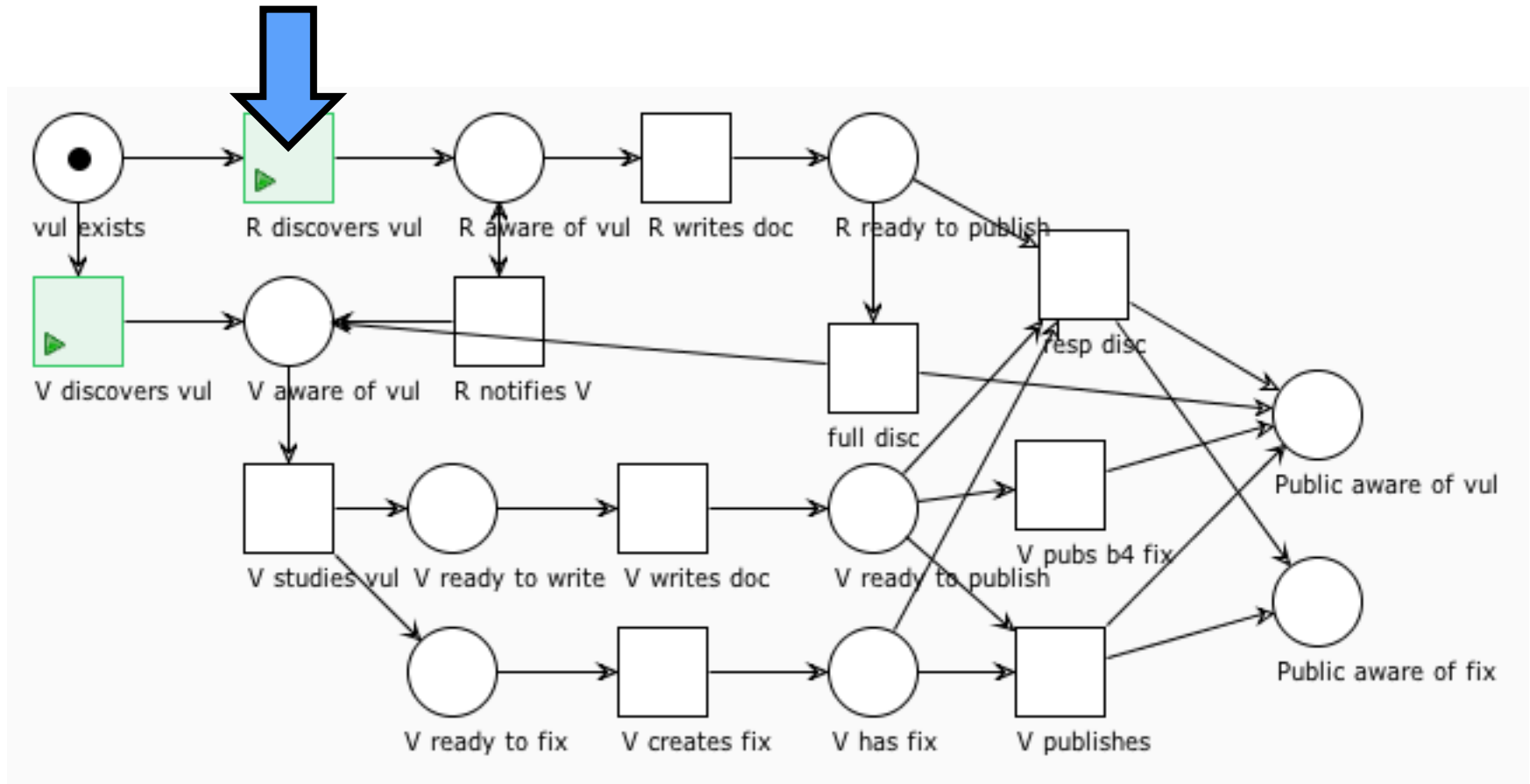
# Vendor Model



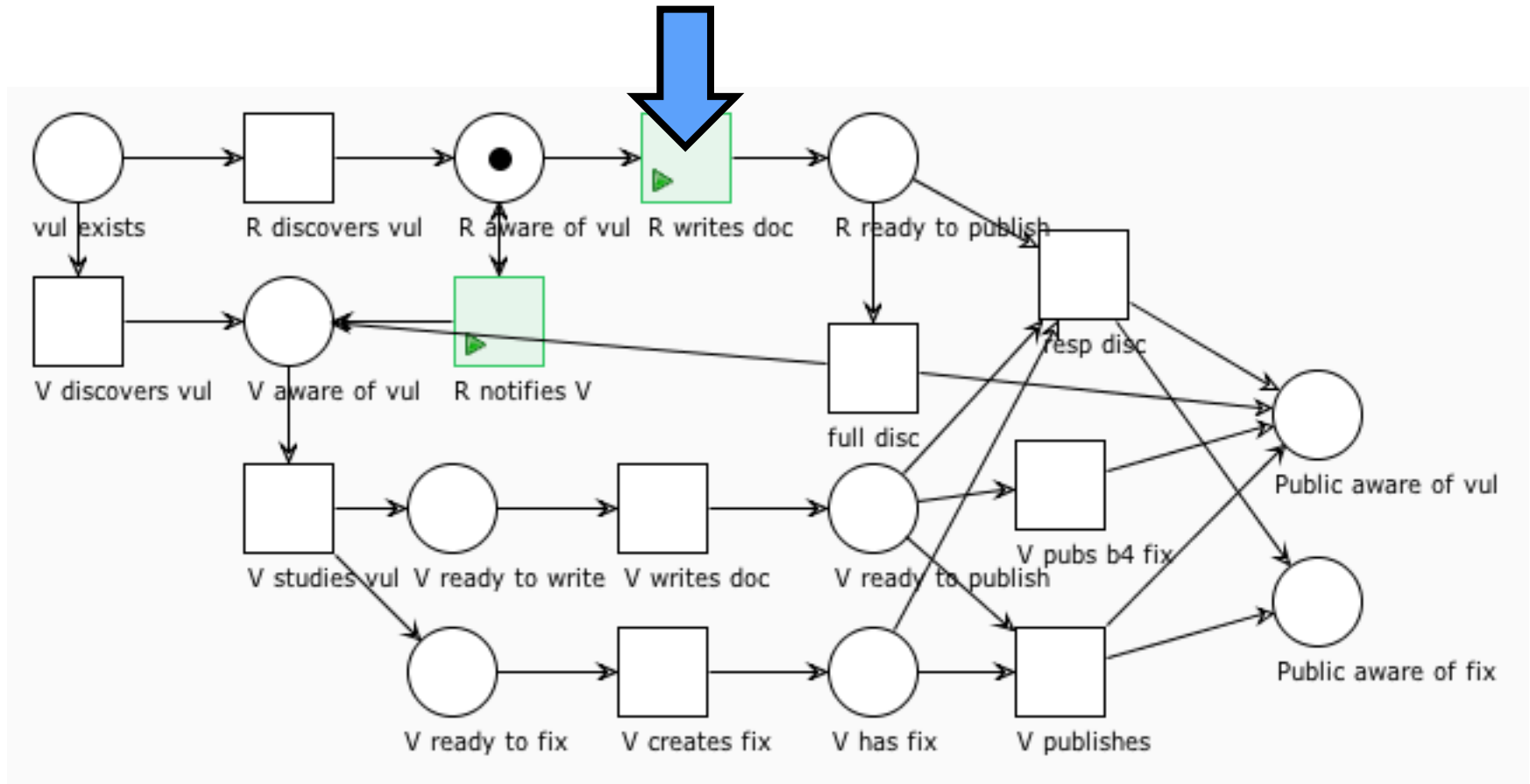
# Vendor + Researcher Model



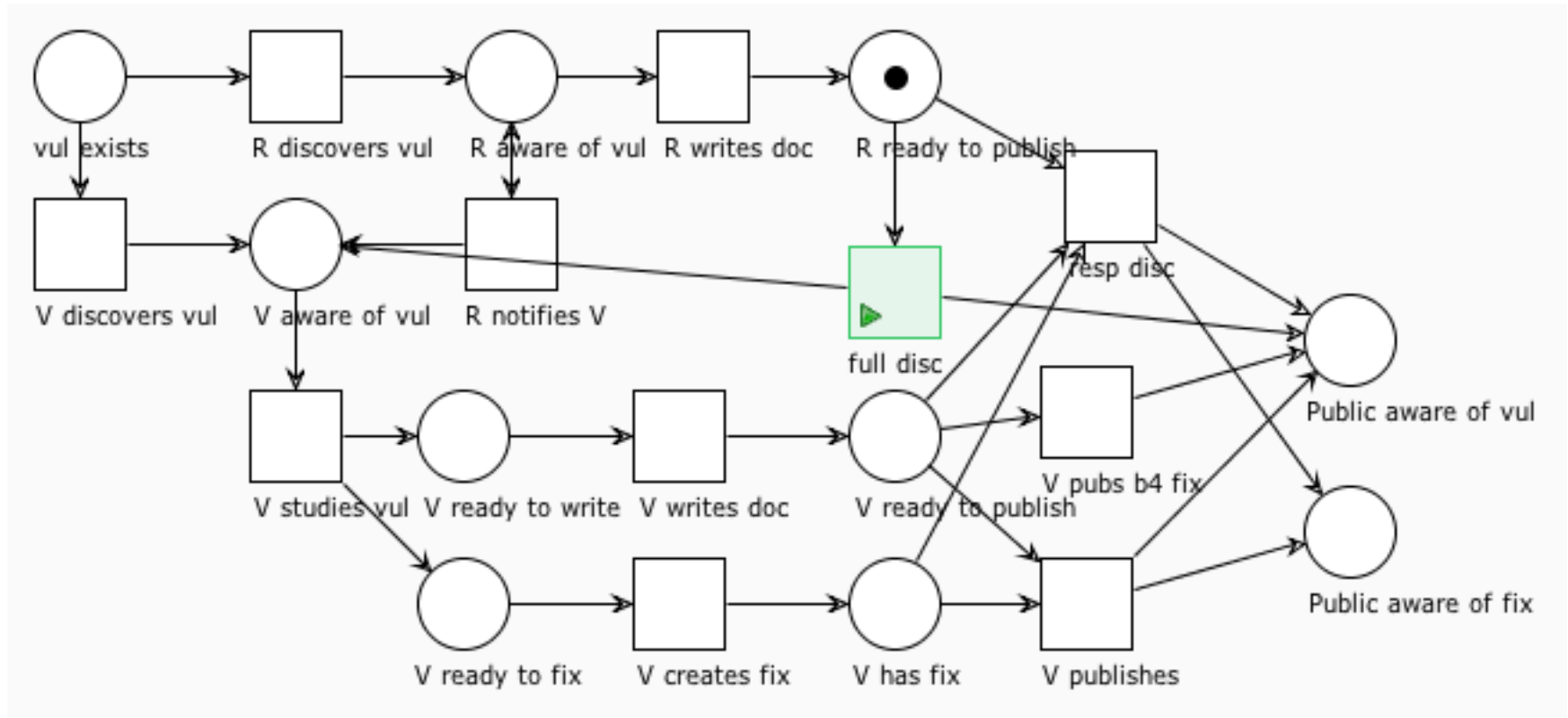
# Vendor + Researcher Model



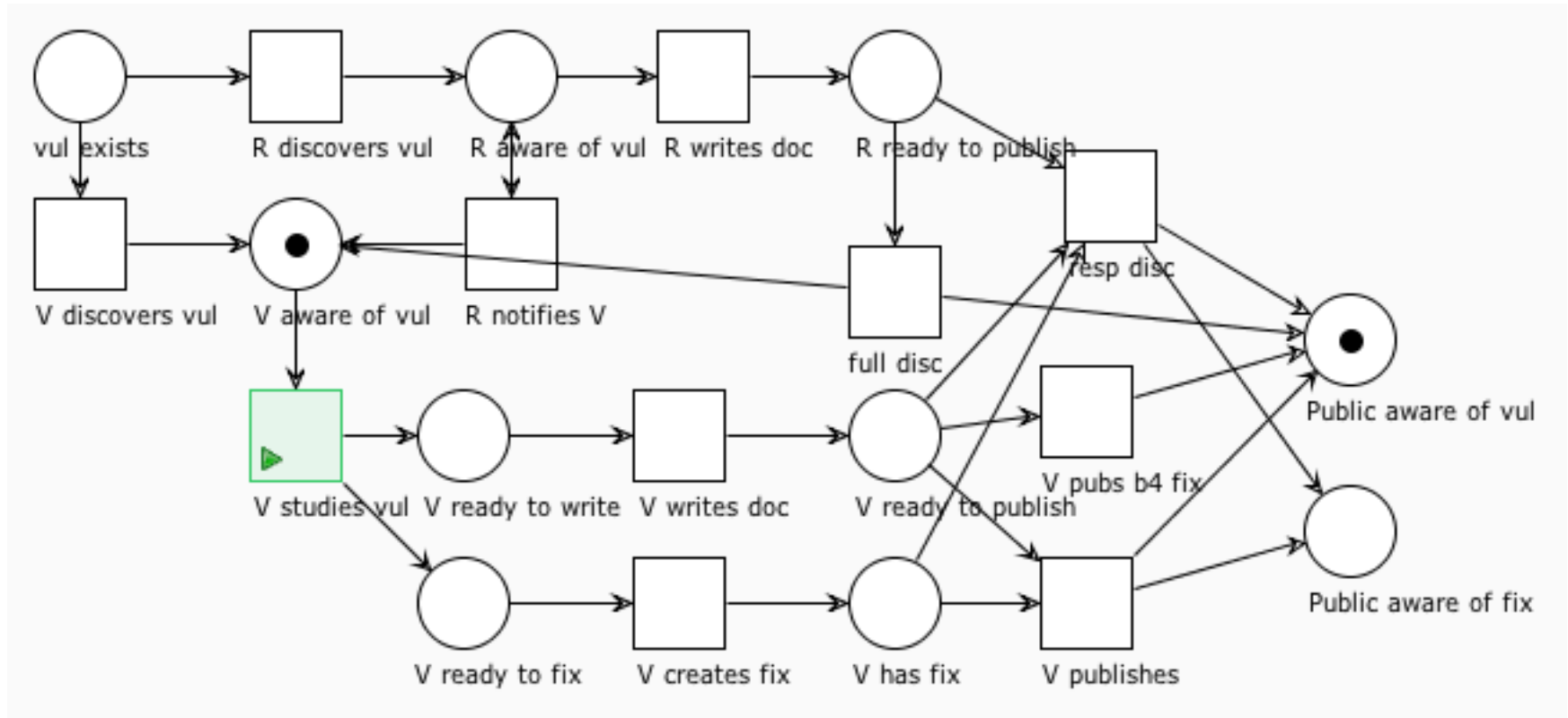
# Vendor + Researcher Model



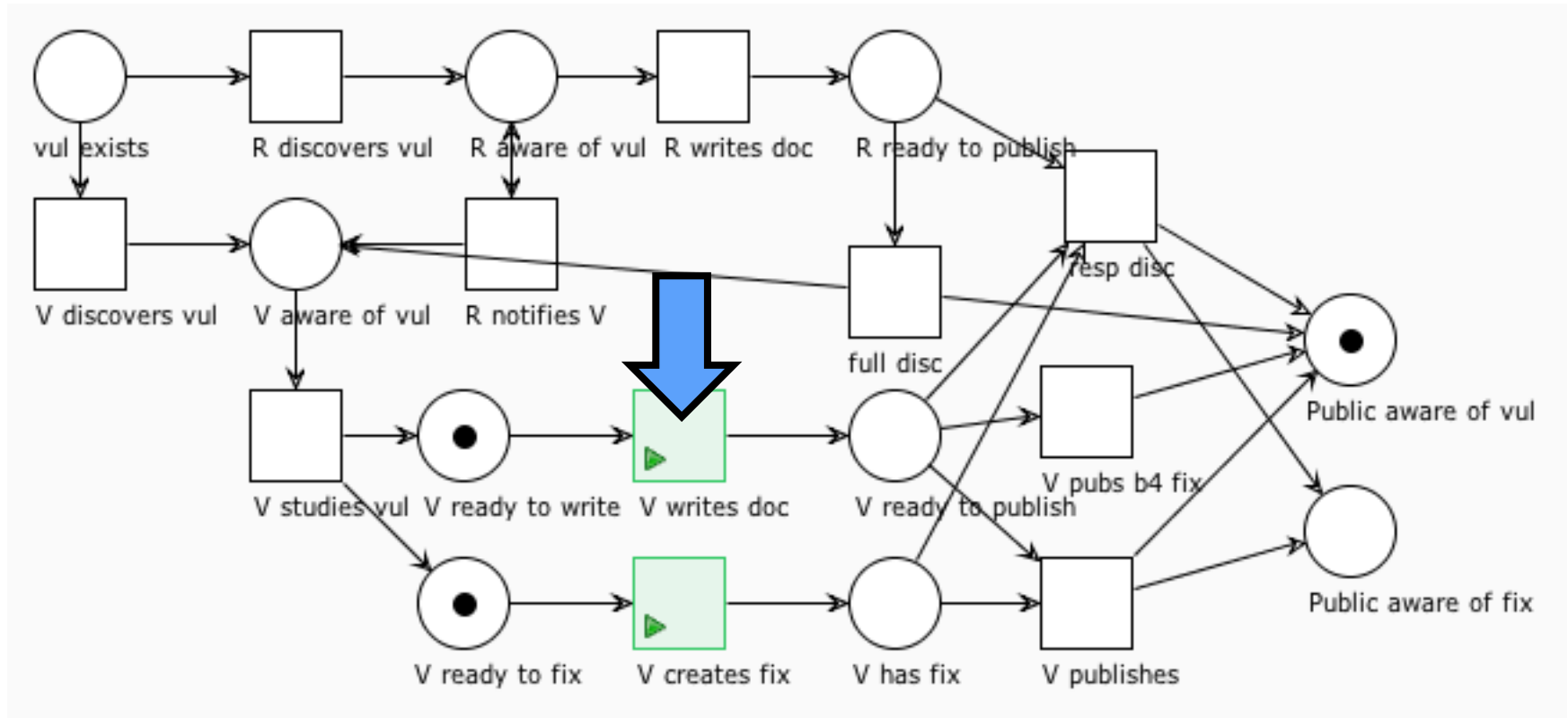
# Vendor + Researcher Model



# Vendor + Researcher Model

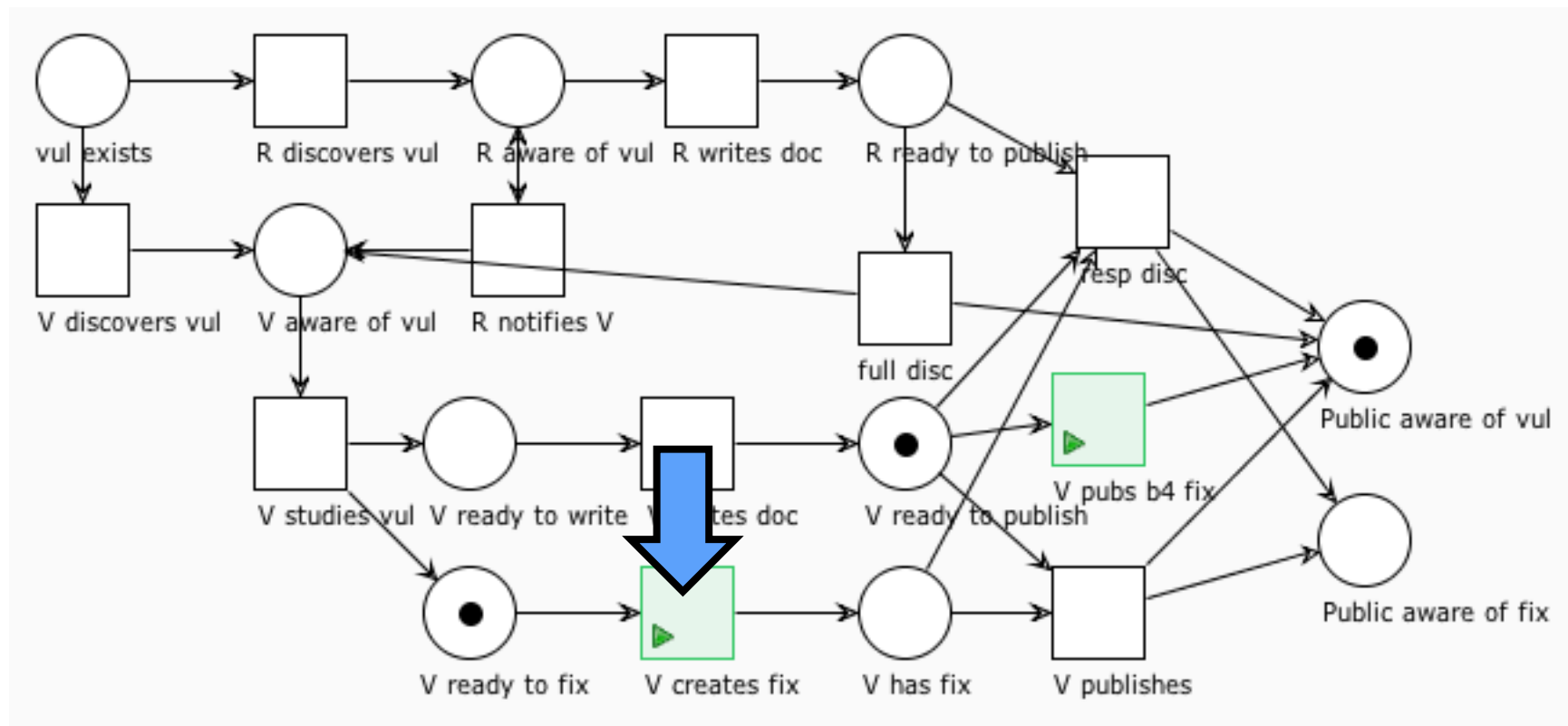


# Vendor + Researcher Model

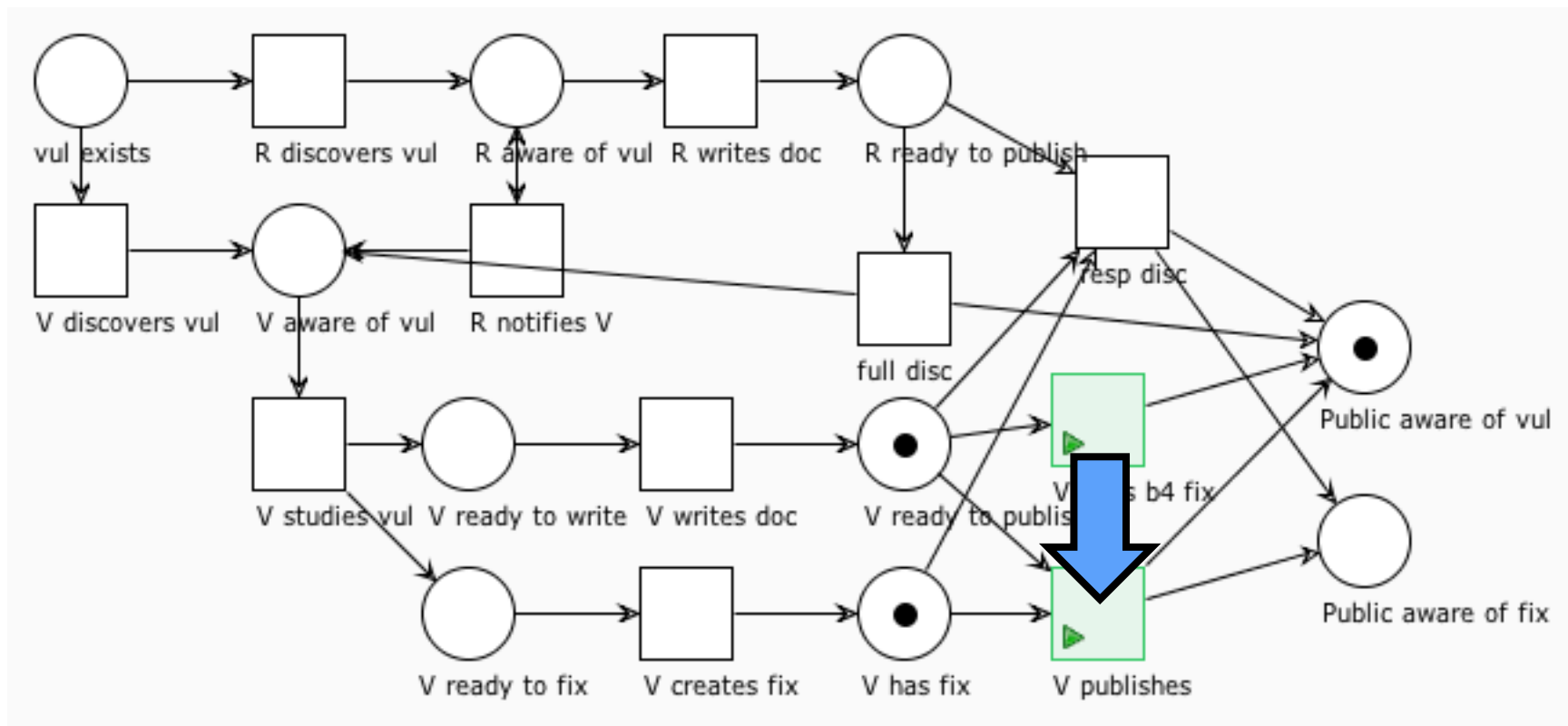




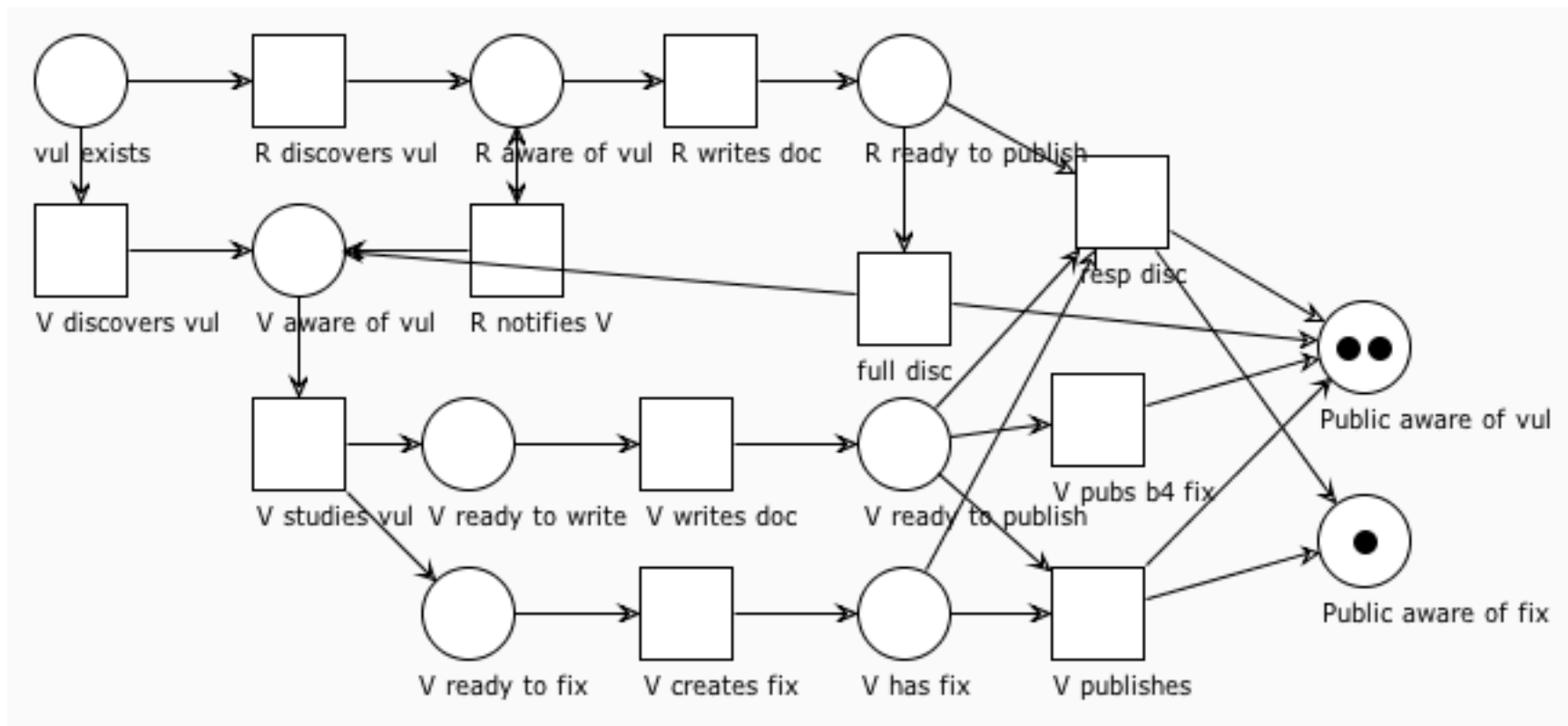
# Vendor + Researcher Model



# Vendor + Researcher Model

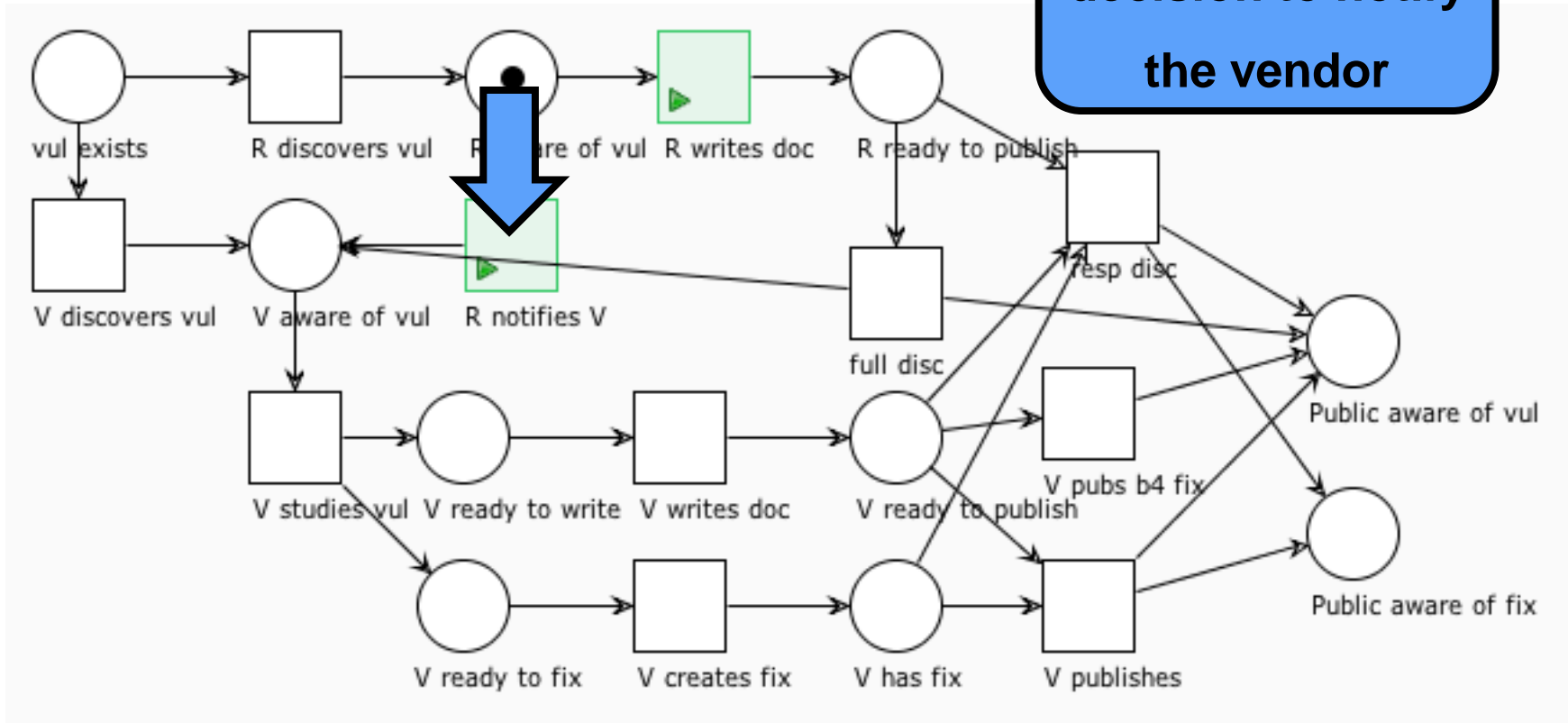


# Vendor + Researcher Model

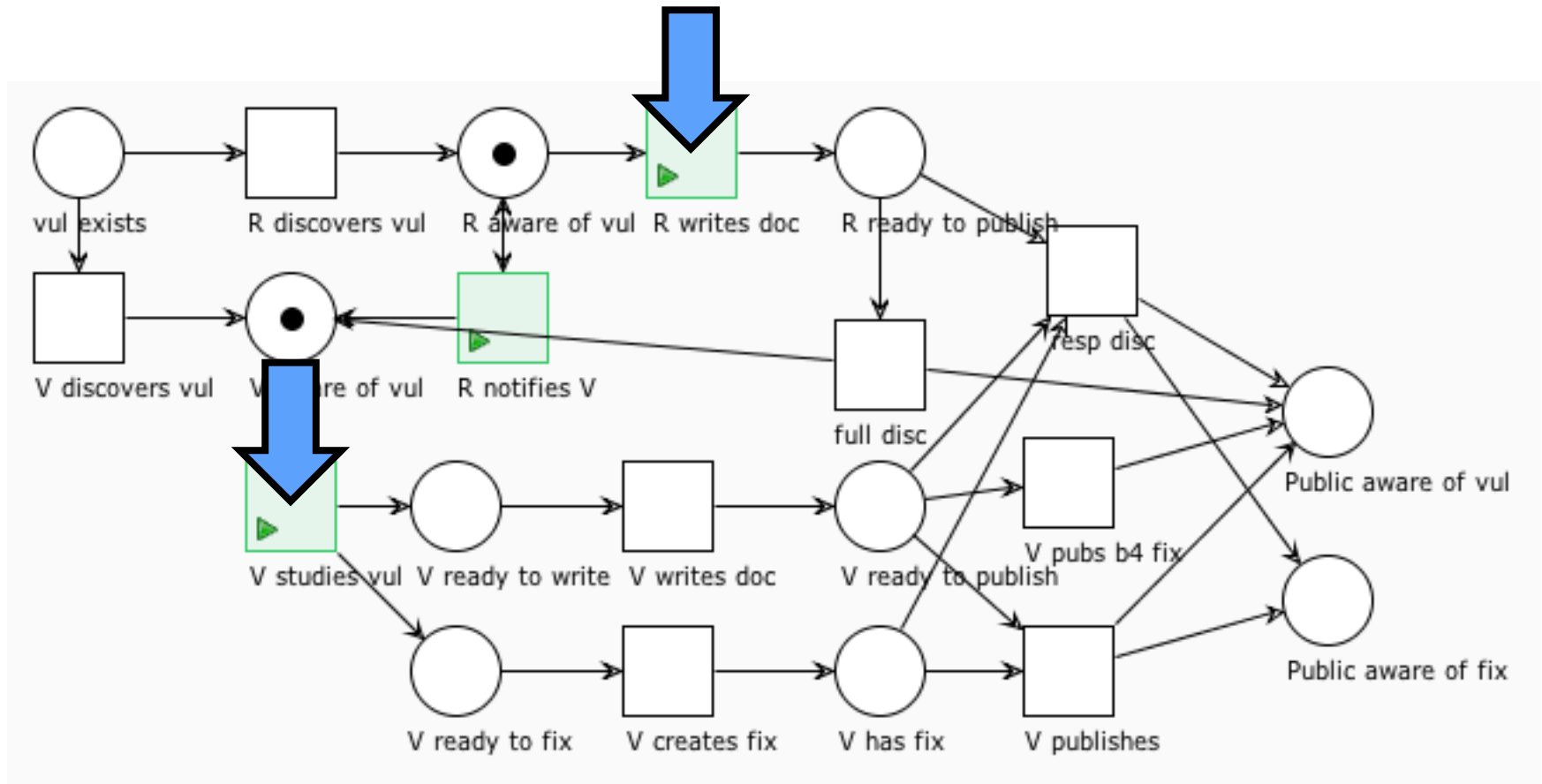


# Vendor + Researcher Model

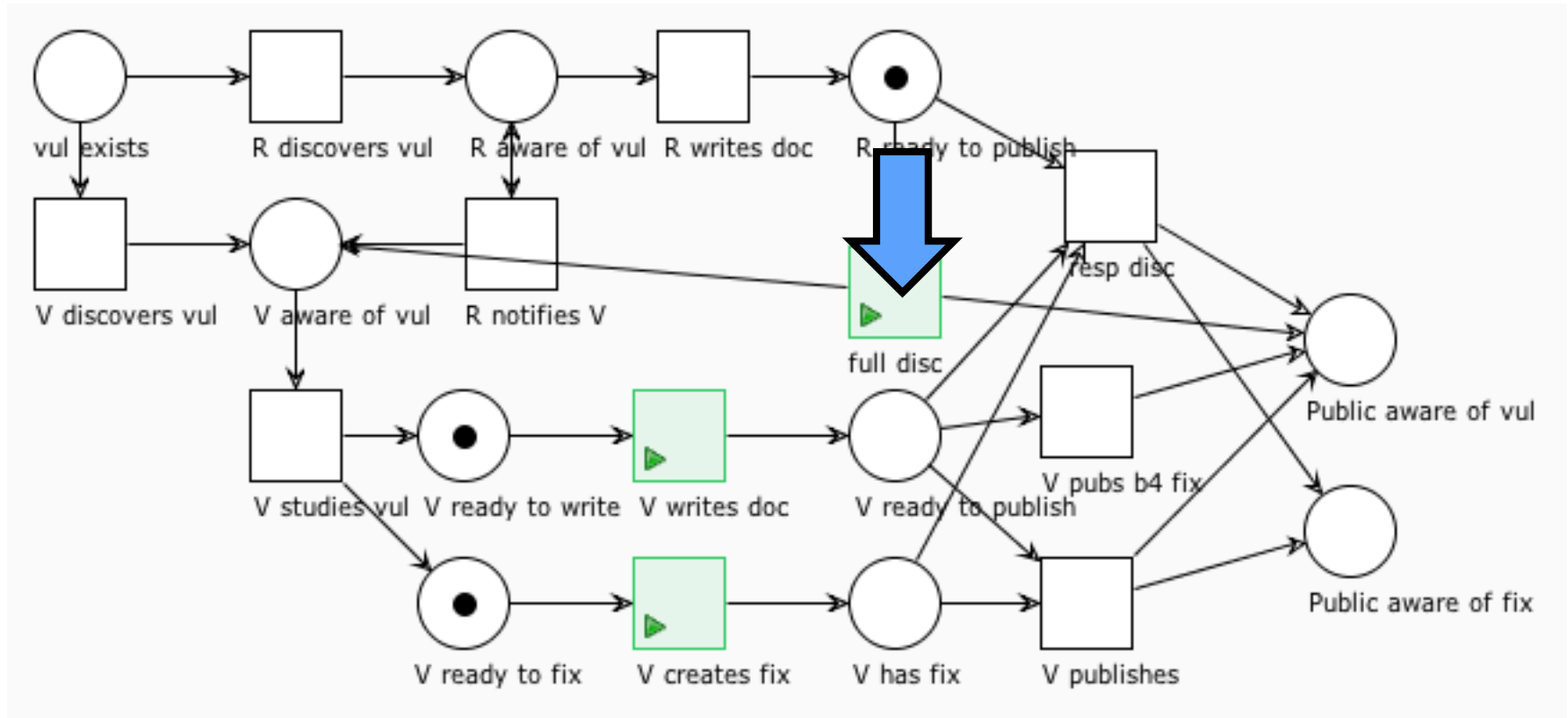
**Rewind to the decision to notify the vendor**



# Vendor + Researcher Model



# Vendor + Researcher Model



# Researcher gives up on vendor, Vendor thought it was fixed



Minecraft / MC-79612

## NBT accounting incorrectly allows for giant allocations

### Timeline

1. 28th July, 2013: First contact with mojang employee about the issue, vulnerability disclosed and proof of concept provided.
2. 19th August, 2013: Second time asking about fix, response given that its being worked on.

“A combination of mis-communication and lack of testing led to this situation today, hopefully it can be a good learning experience.”

Confirmation Status: Unconfirmed

proper testing.

### Description

Stolen from <http://blog.ammaraskar.com/minecraft-vulnerability-advisory/>

#### A lesson on data structures, networking protocols, data sanitization and disclosure

Around 2 years ago, I was enthusiastically working on Spigot and Bukkit along with a couple of fairly popular plugins. During my poking around within the networking internals of Minecraft, I came across a fairly substantial problem that allowed anyone to send certain malformed packets and crash a server by running it out of memory.

Following the defacto standard procedure, I responsibly and privately disclosed the problem to Mojang on 10th July, 2013. That's nearly 2 years ago. I asked for updates in one month intervals over the course of 3 months and was ignored or given highly unsatisfactory responses. I kept my hopes up that the problem would be patched and checked the source code on new releases whenever I could.

The version of the game when the vulnerability was reported was 1.6.2, the game is now on version 1.8.3. That's right, 2 major versions and dozens of minor versions and a critical

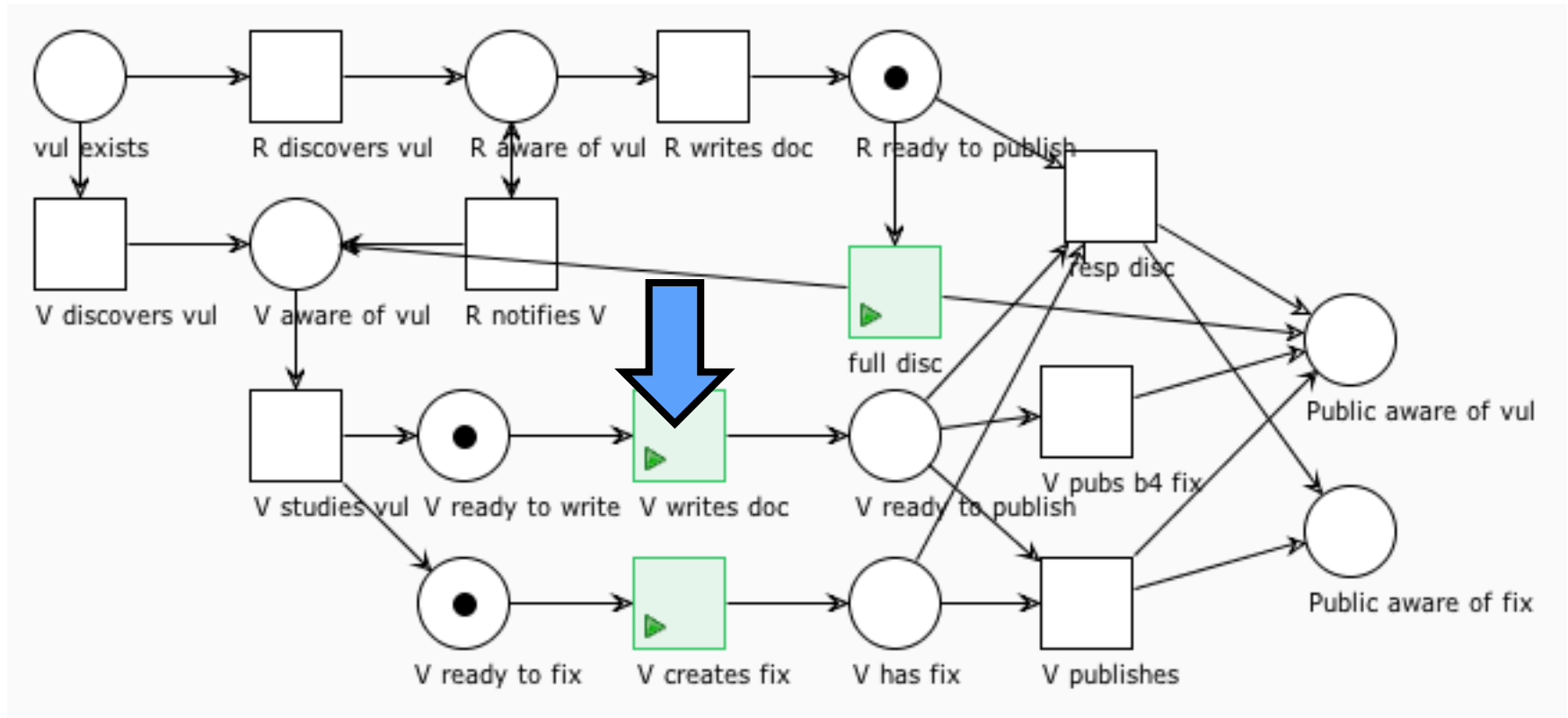
### Activity

All Comments History Activity Transitions Summary

violine1101 added a comment - 17/Apr/15 7:43 PM

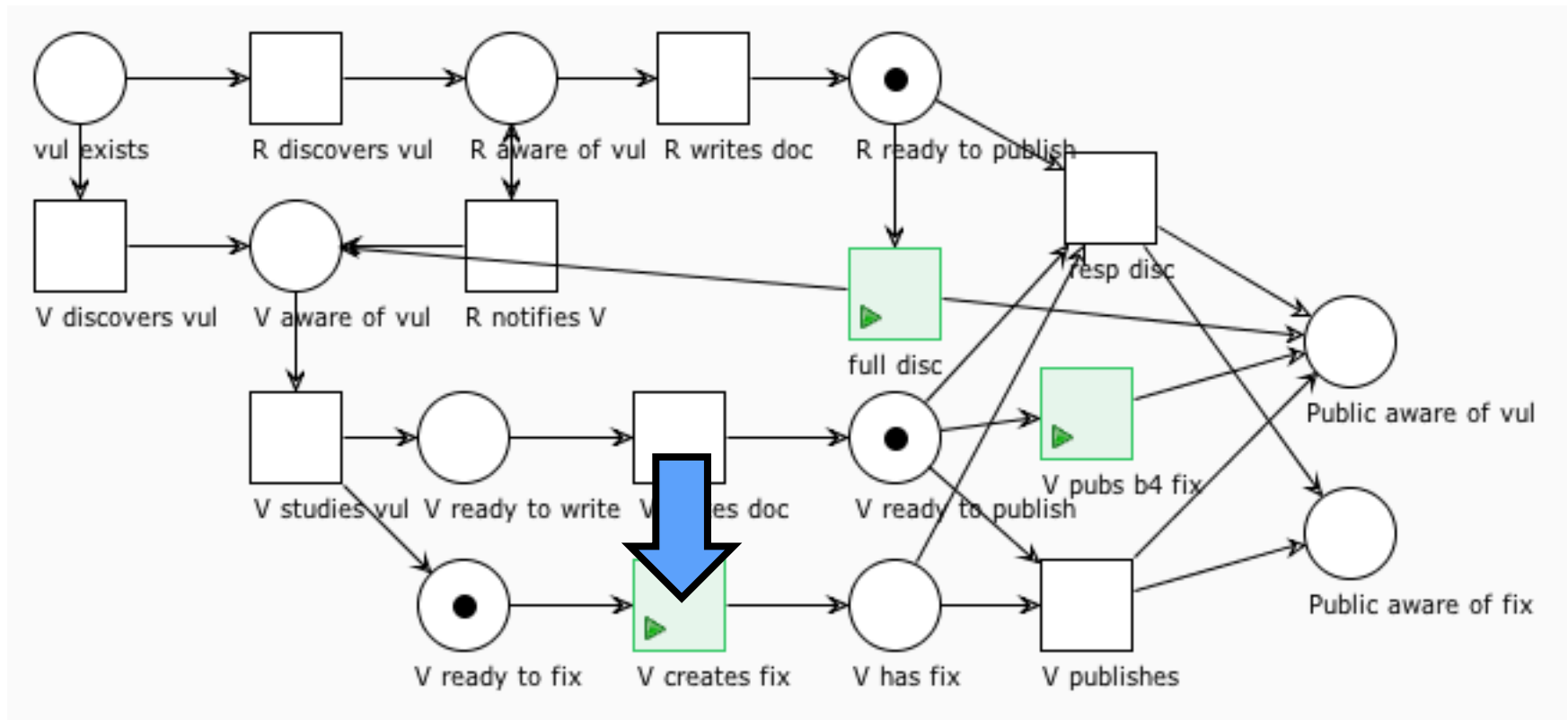
From <http://blog.ammaraskar.com/minecraft-vulnerability-advisory/>  
*Update 2:* The exact problem that caused this bug to go unpatched has been identified. Mojang attempted to implement a fix for this problem, however they did not test their fix against the proof of concept I provided, which still crashed the server perfectly fine. This, in combination with ignoring me when I asked for status updates twice led me to believe that Mojang had attempted no fix. In retrospect, a final warning before this full disclosure more recently was probably in order. A combination of mis-communication and lack of testing led to this situation today, hopefully it can be a good learning experience.

# Vendor + Researcher Model

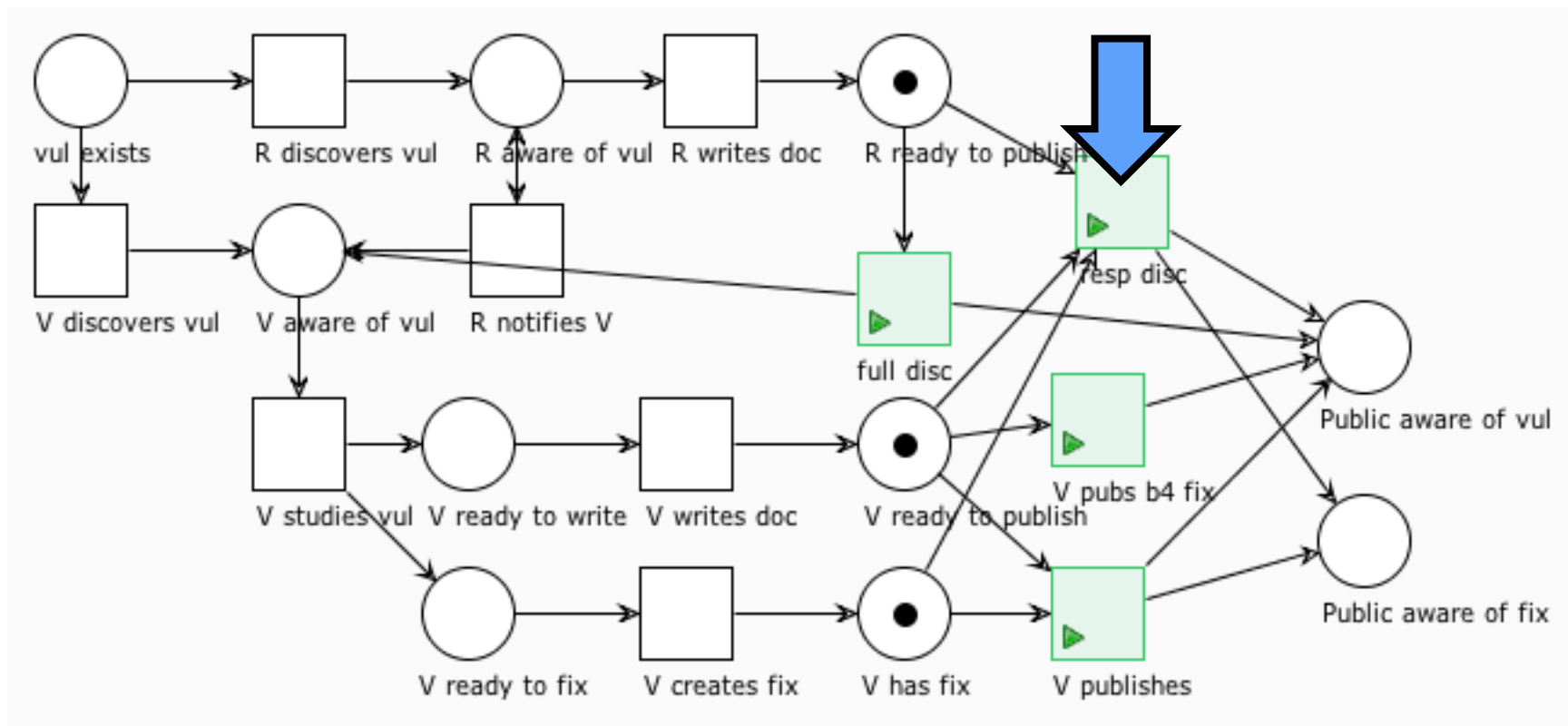




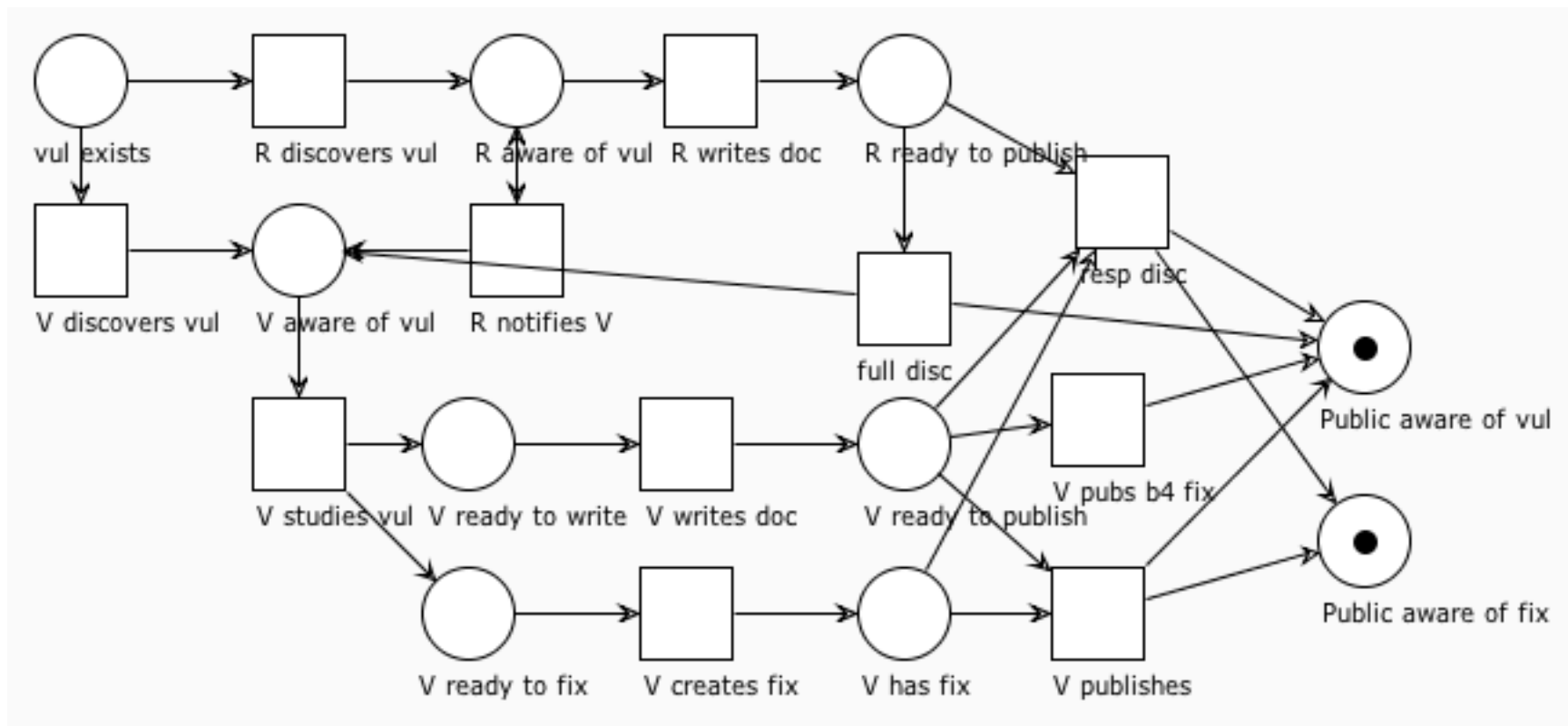
# Vendor + Researcher Model



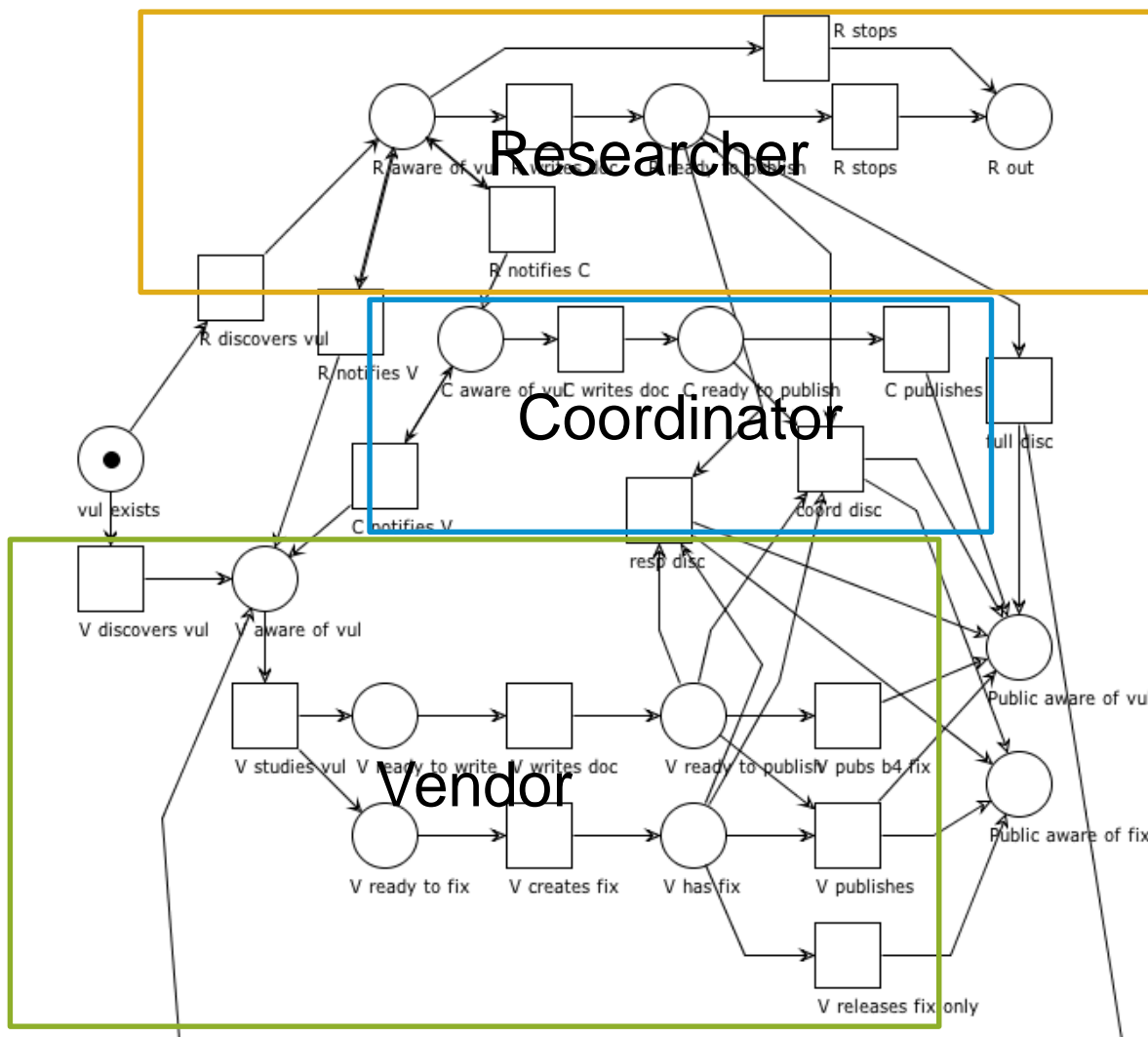
# Vendor + Researcher Model



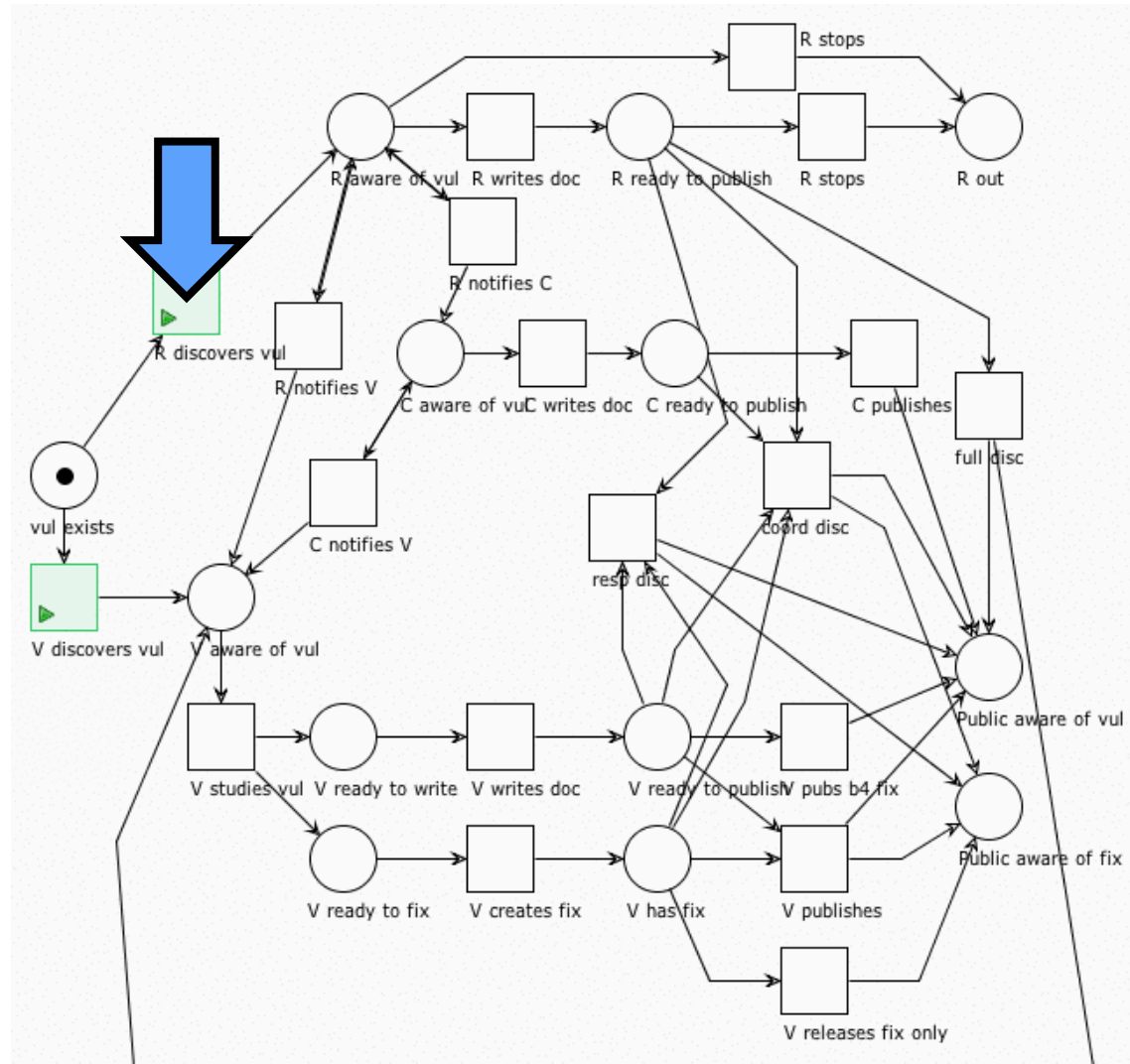
# Vendor + Researcher Model



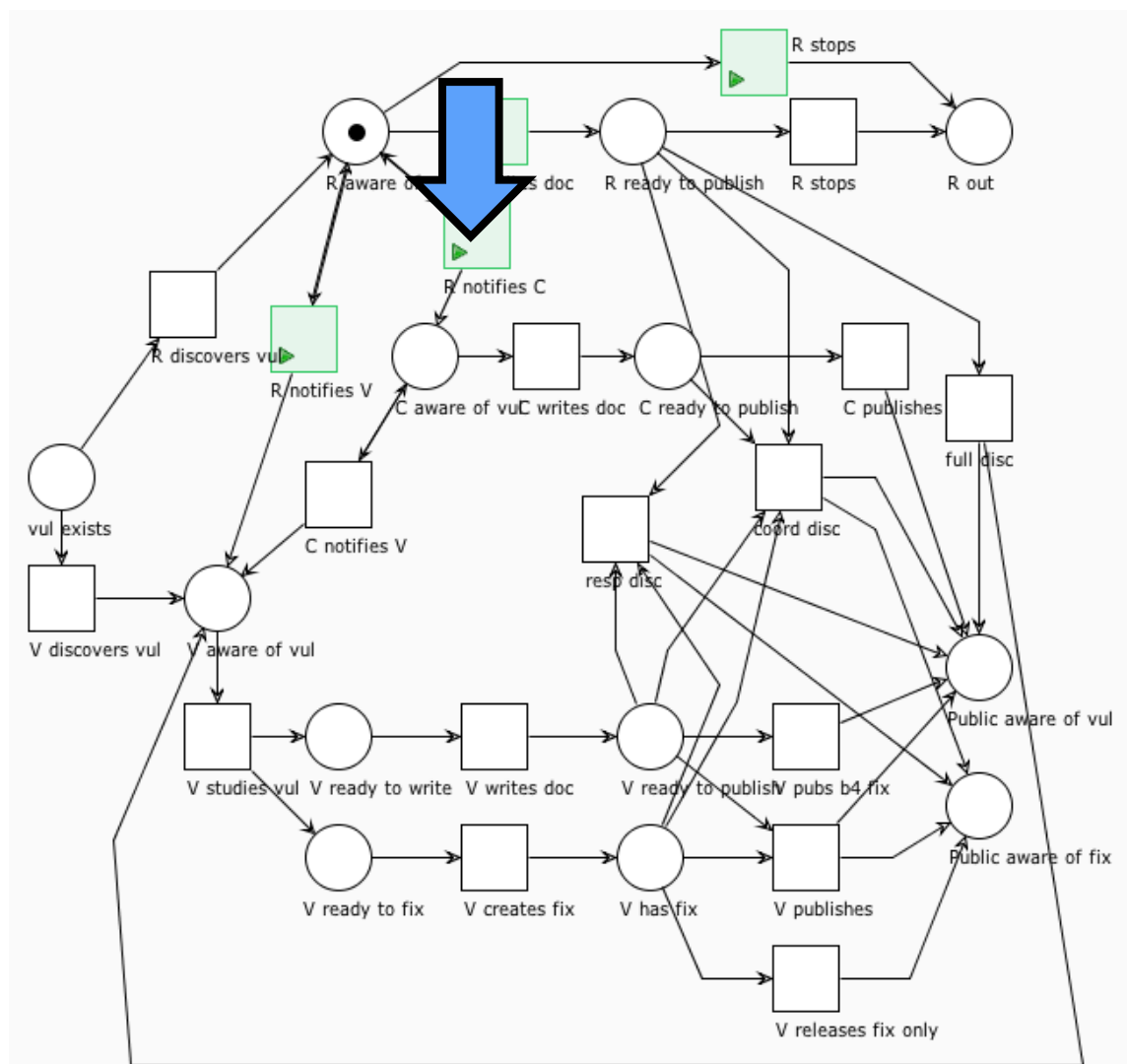
# Vendor, Researcher, Coordinator



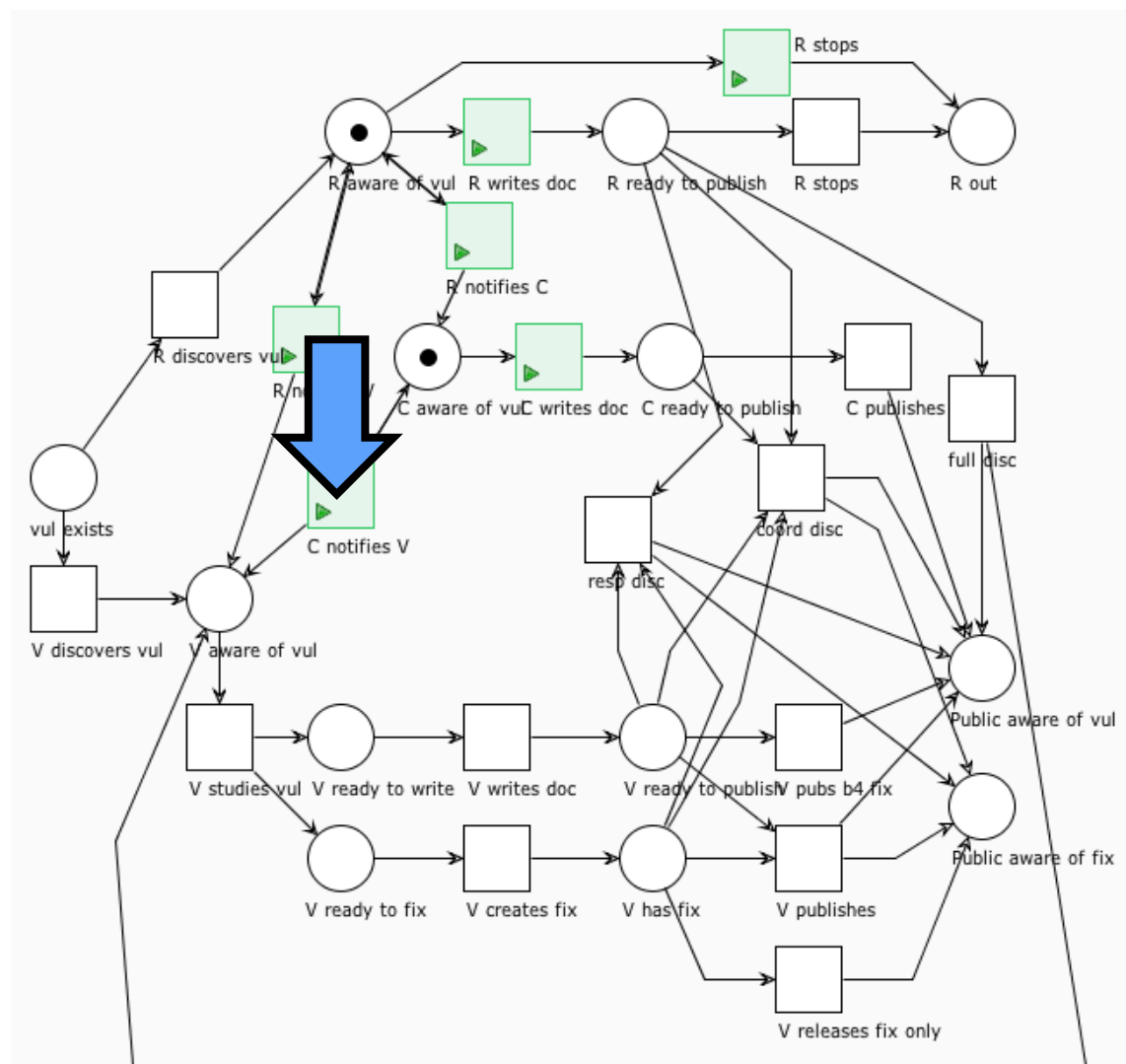
# Vendor, Researcher, Coordinator



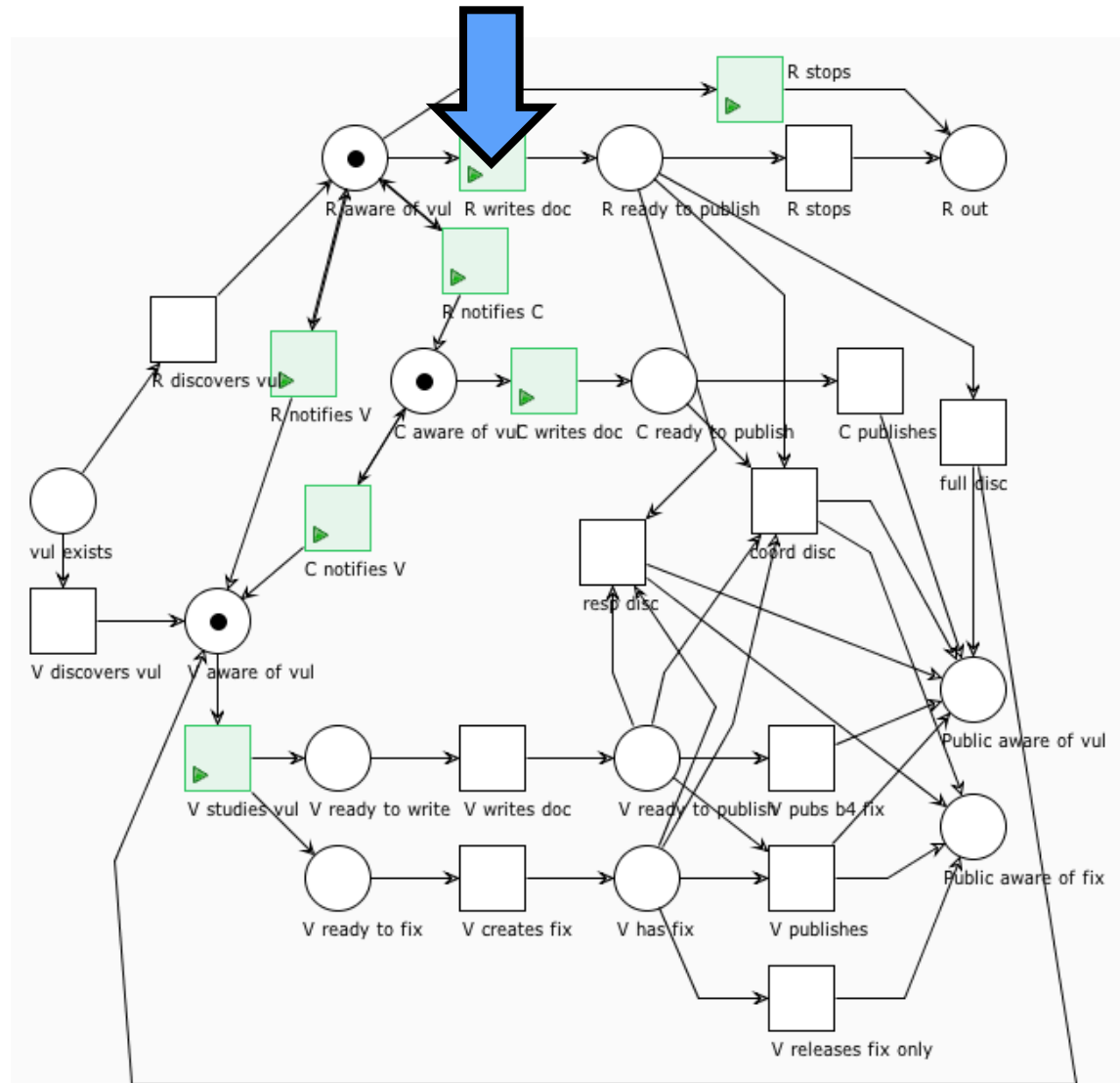
# Vendor, Researcher, Coordinator



# Vendor, Researcher, Coordinator

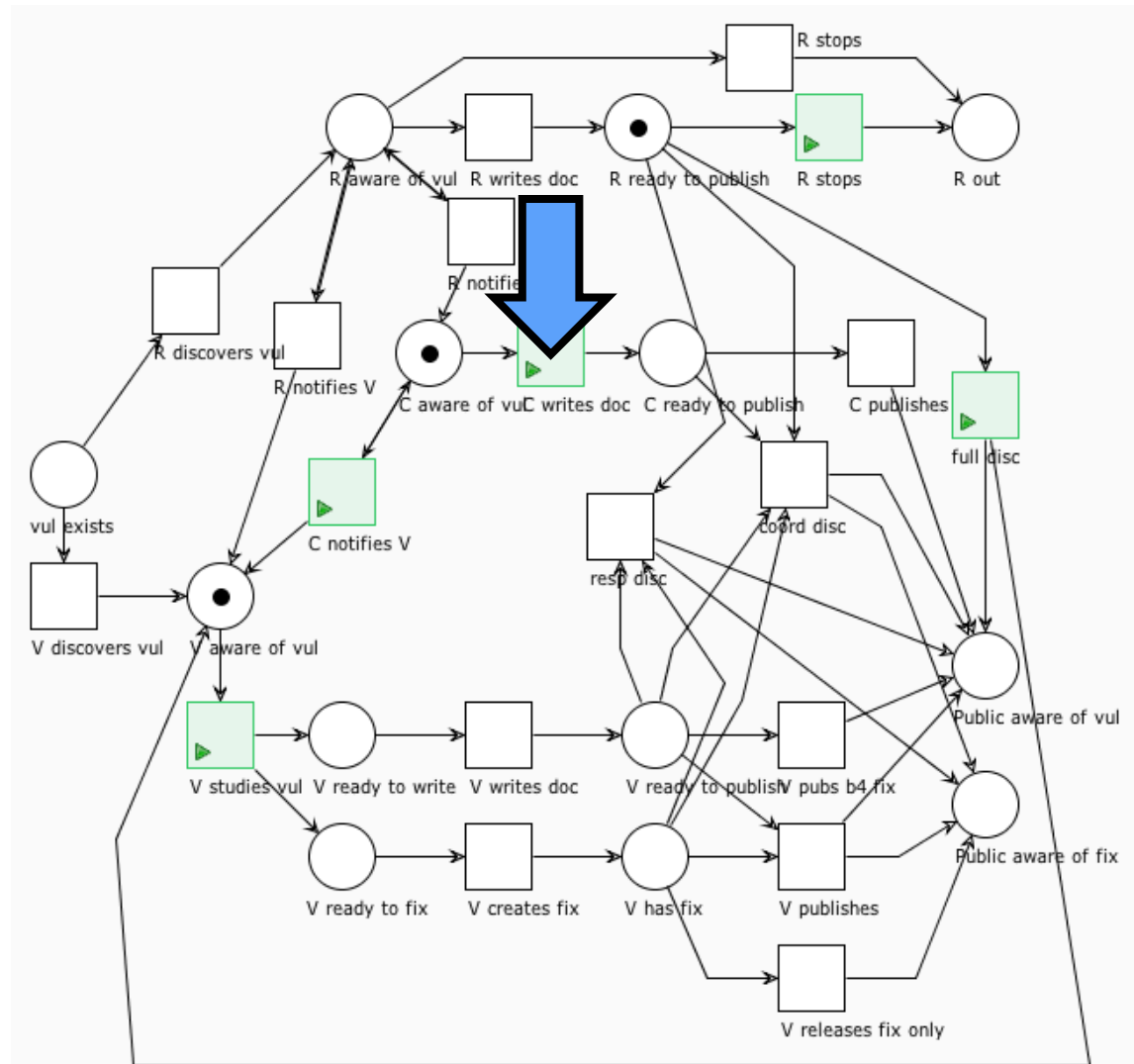


# Vendor, Researcher, Coordinator

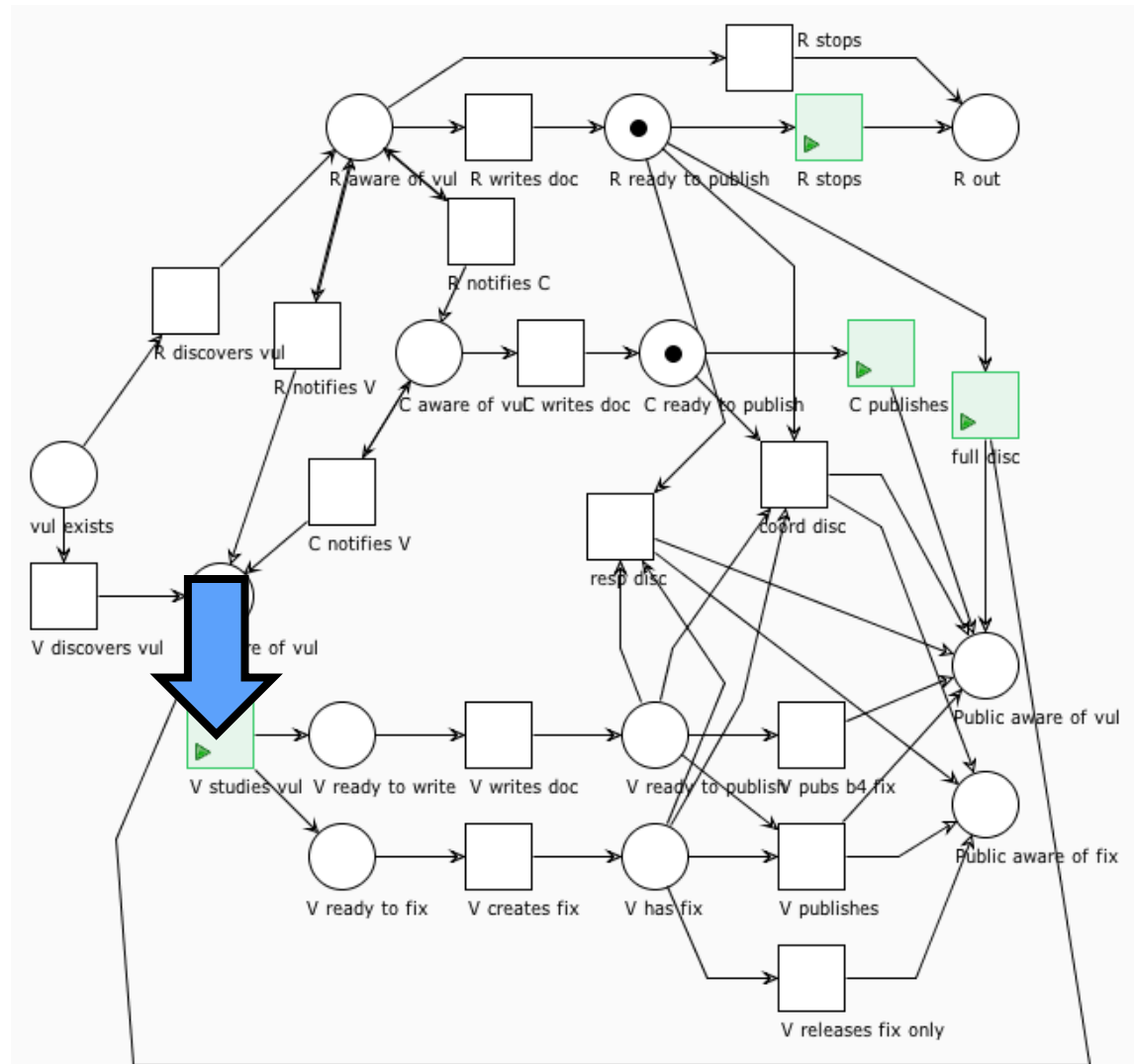




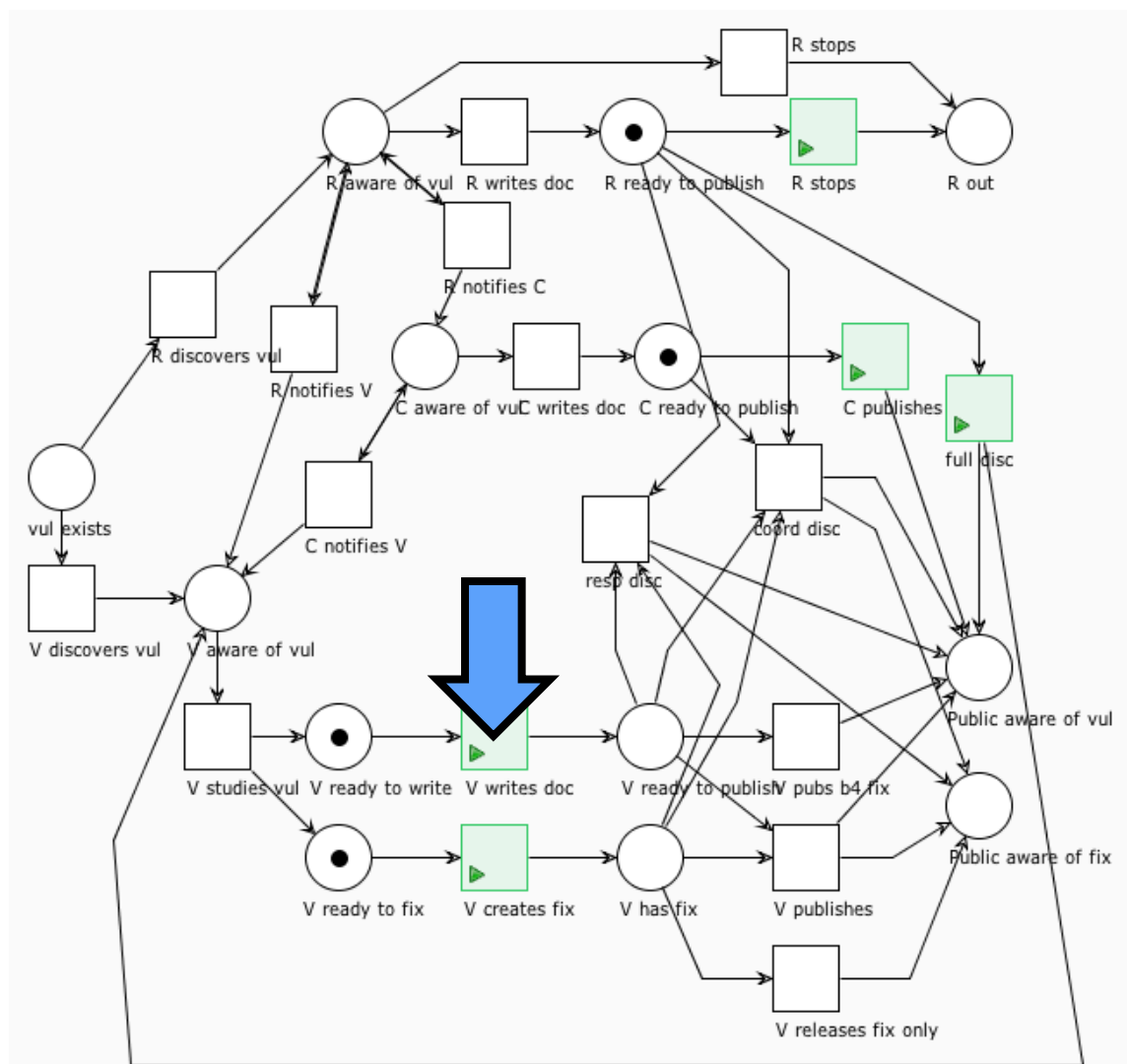
# Vendor, Researcher, Coordinator



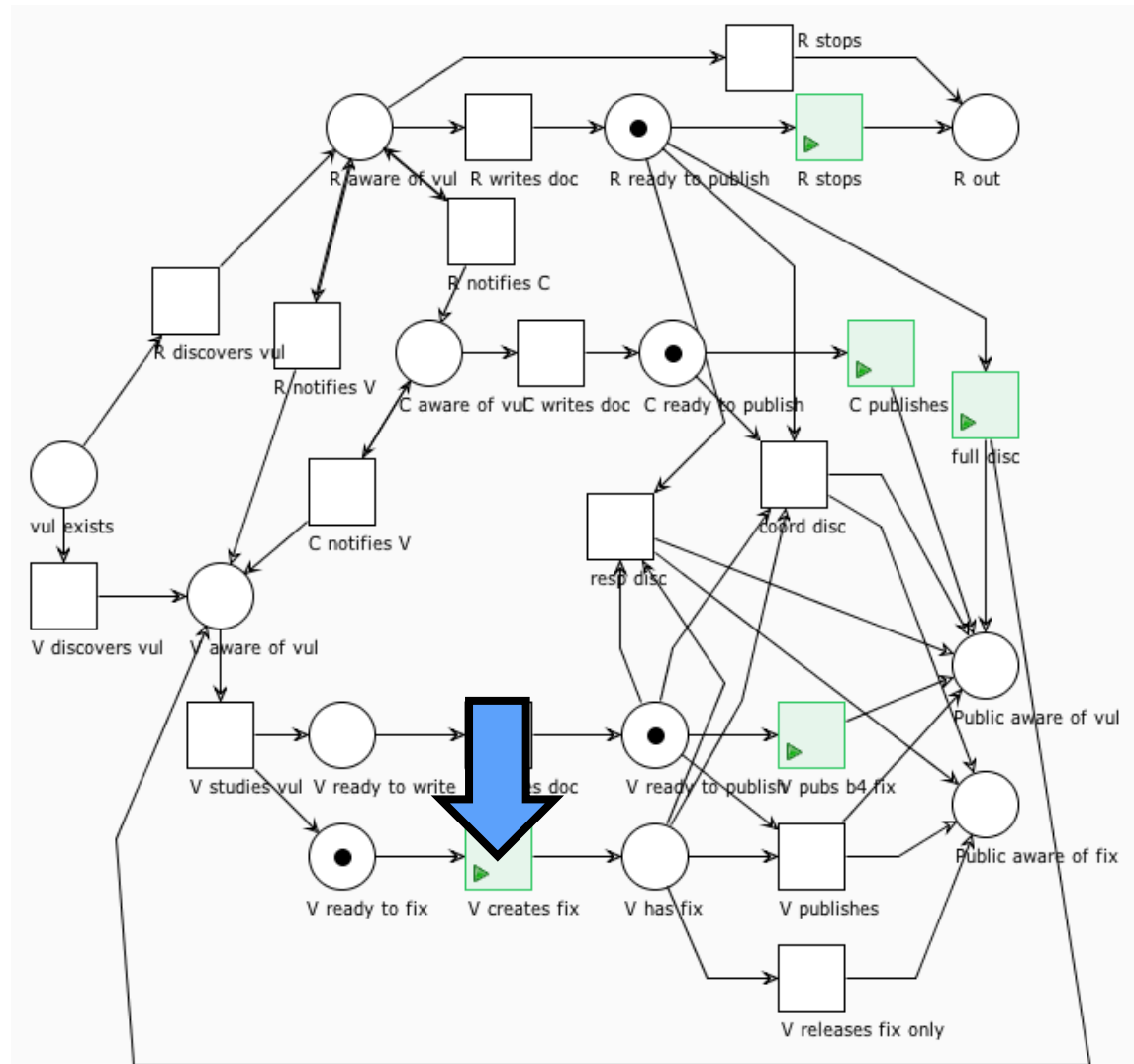
# Vendor, Researcher, Coordinator



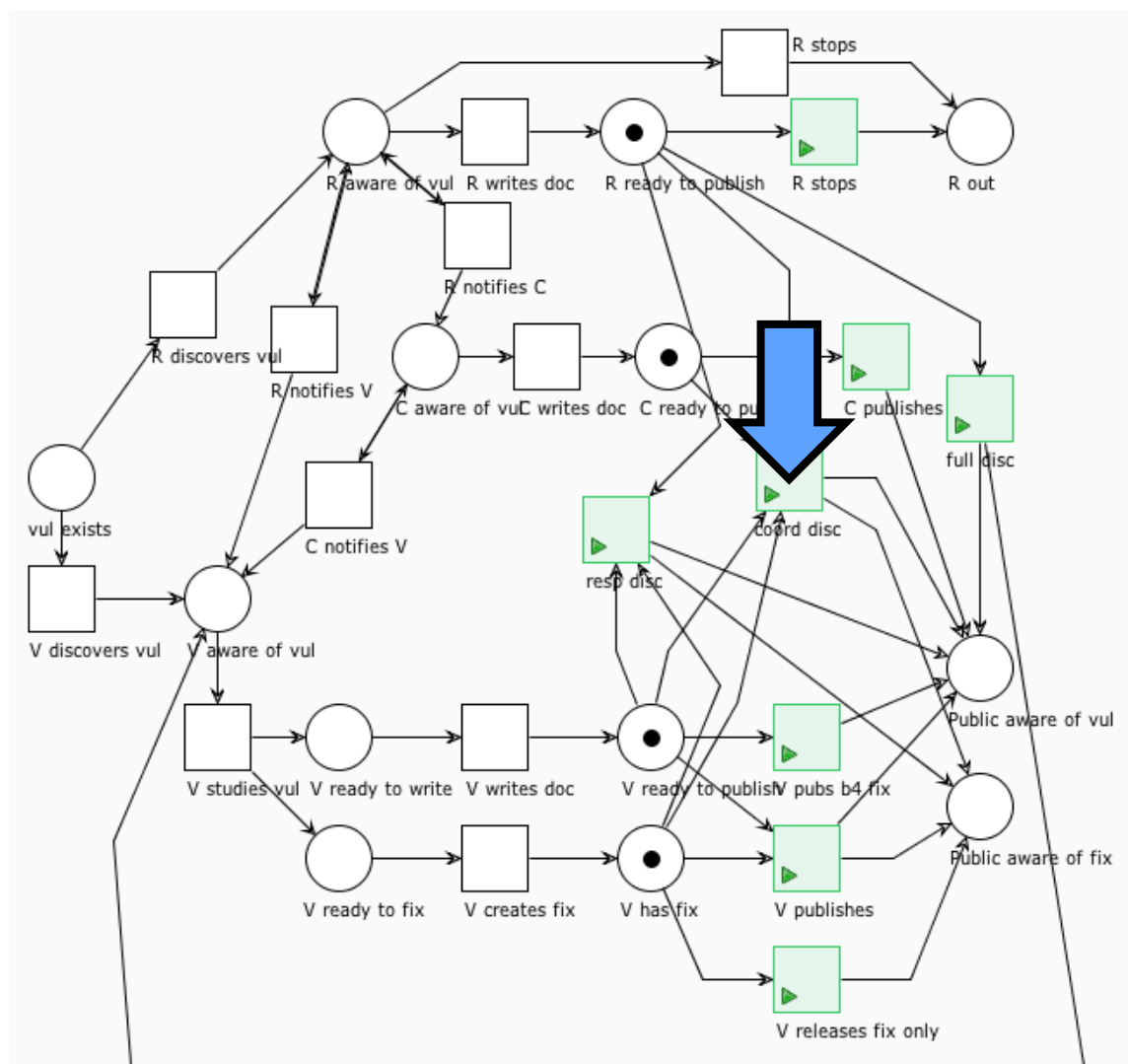
# Vendor, Researcher, Coordinator



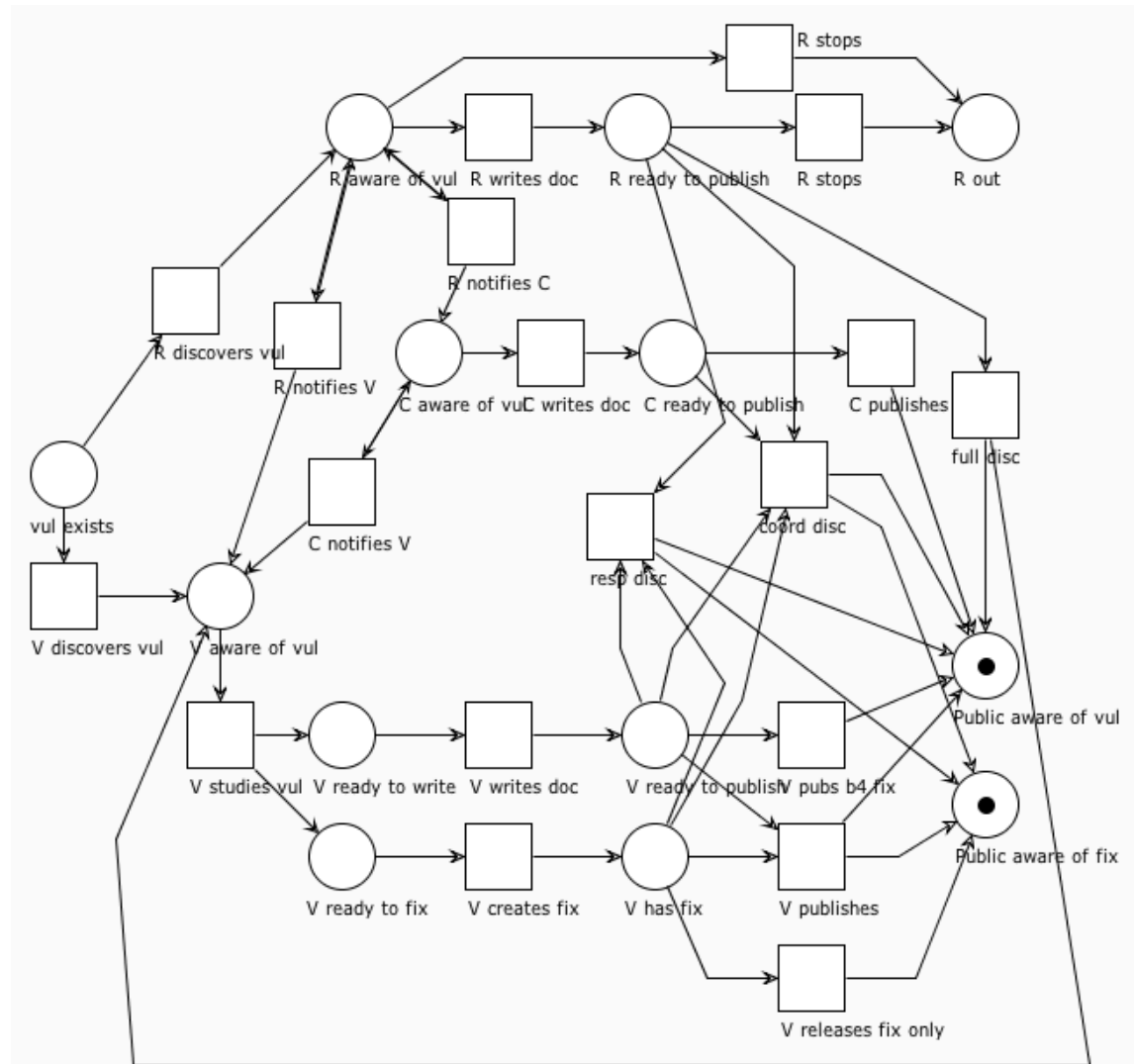
# Vendor, Researcher, Coordinator



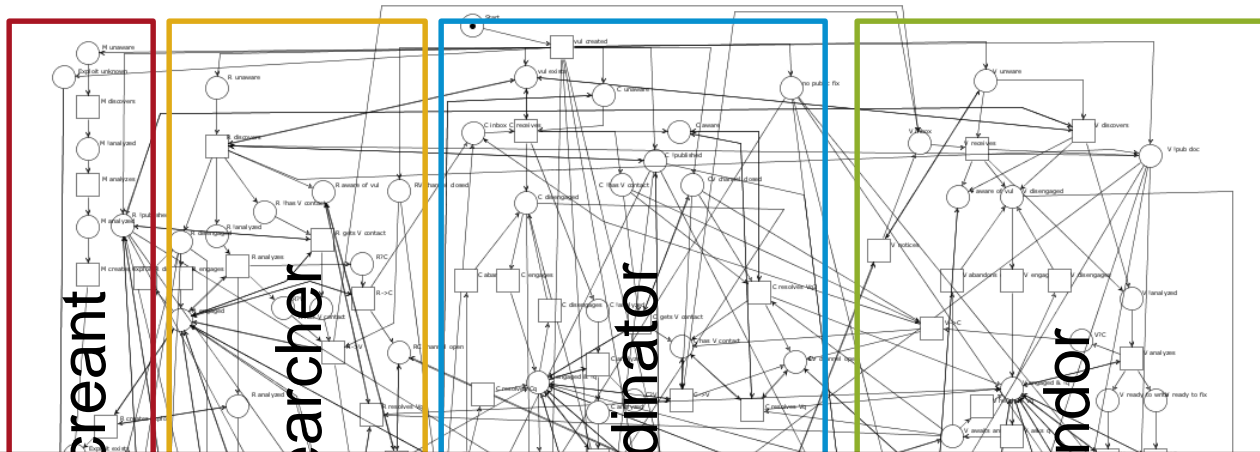
# Vendor, Researcher, Coordinator



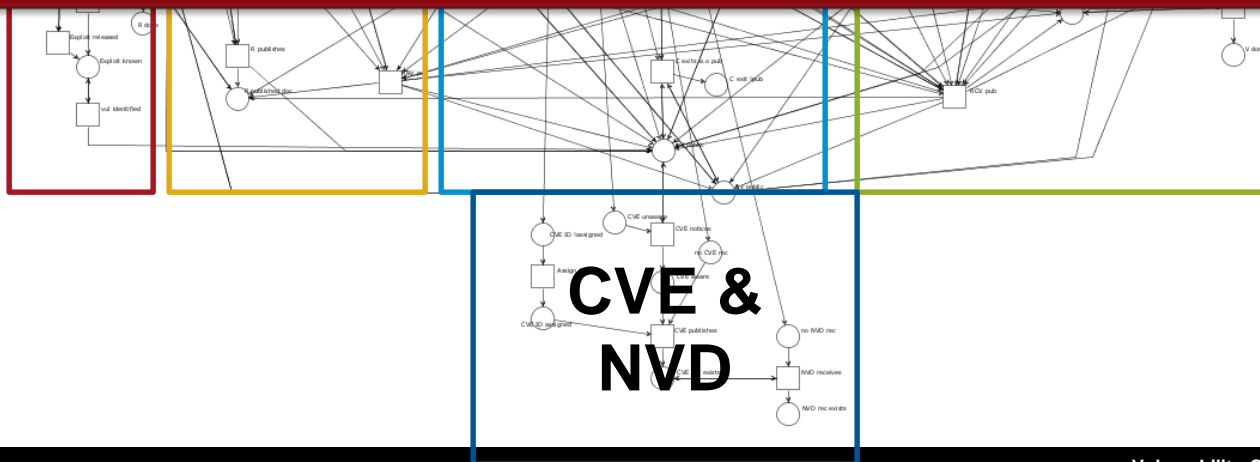
# Vendor, Researcher, Coordinator



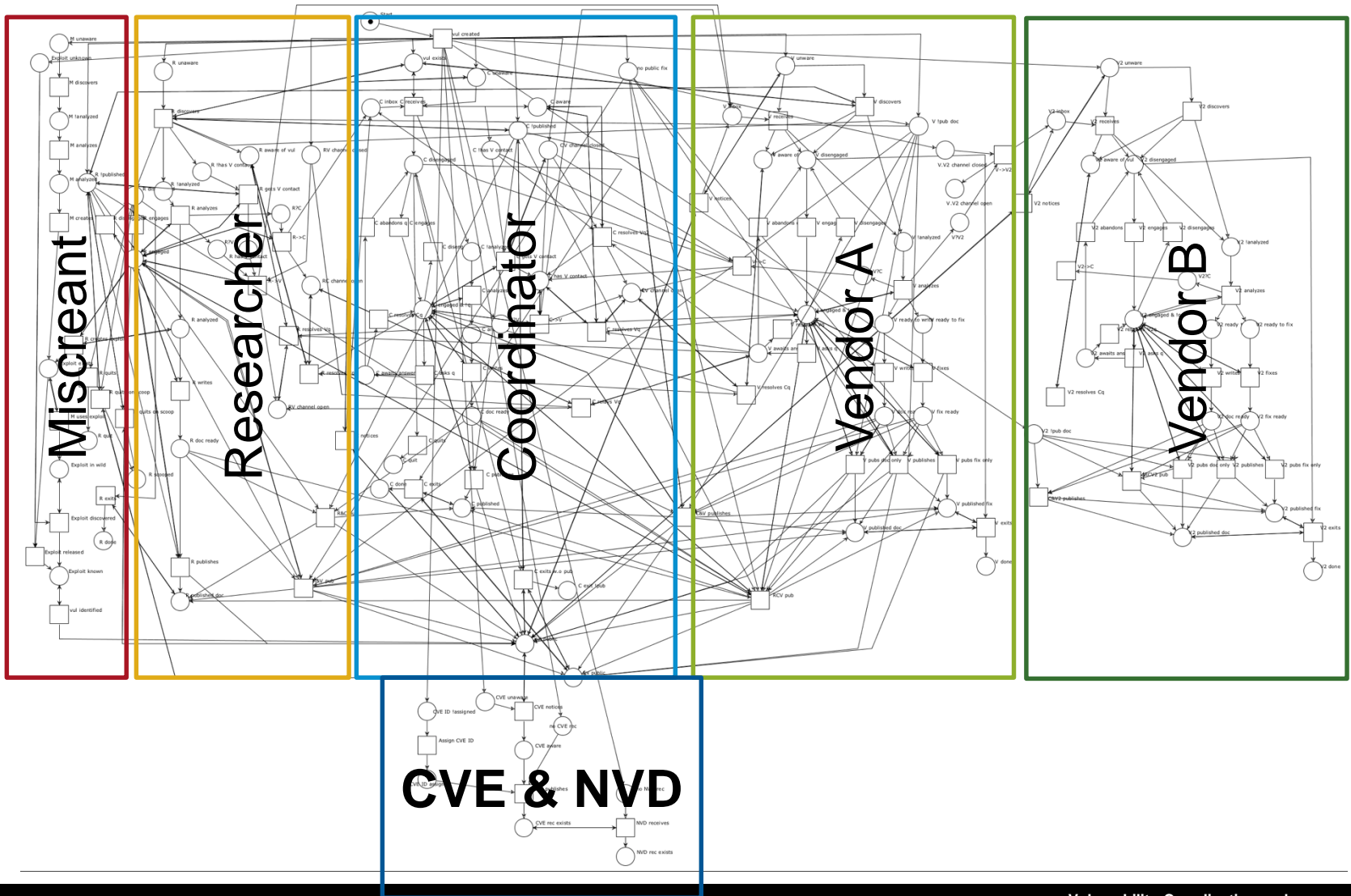
# Vendor, Researcher, Coordinator, Miscreant



**But this is still just a single vendor vulnerability**

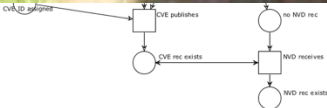
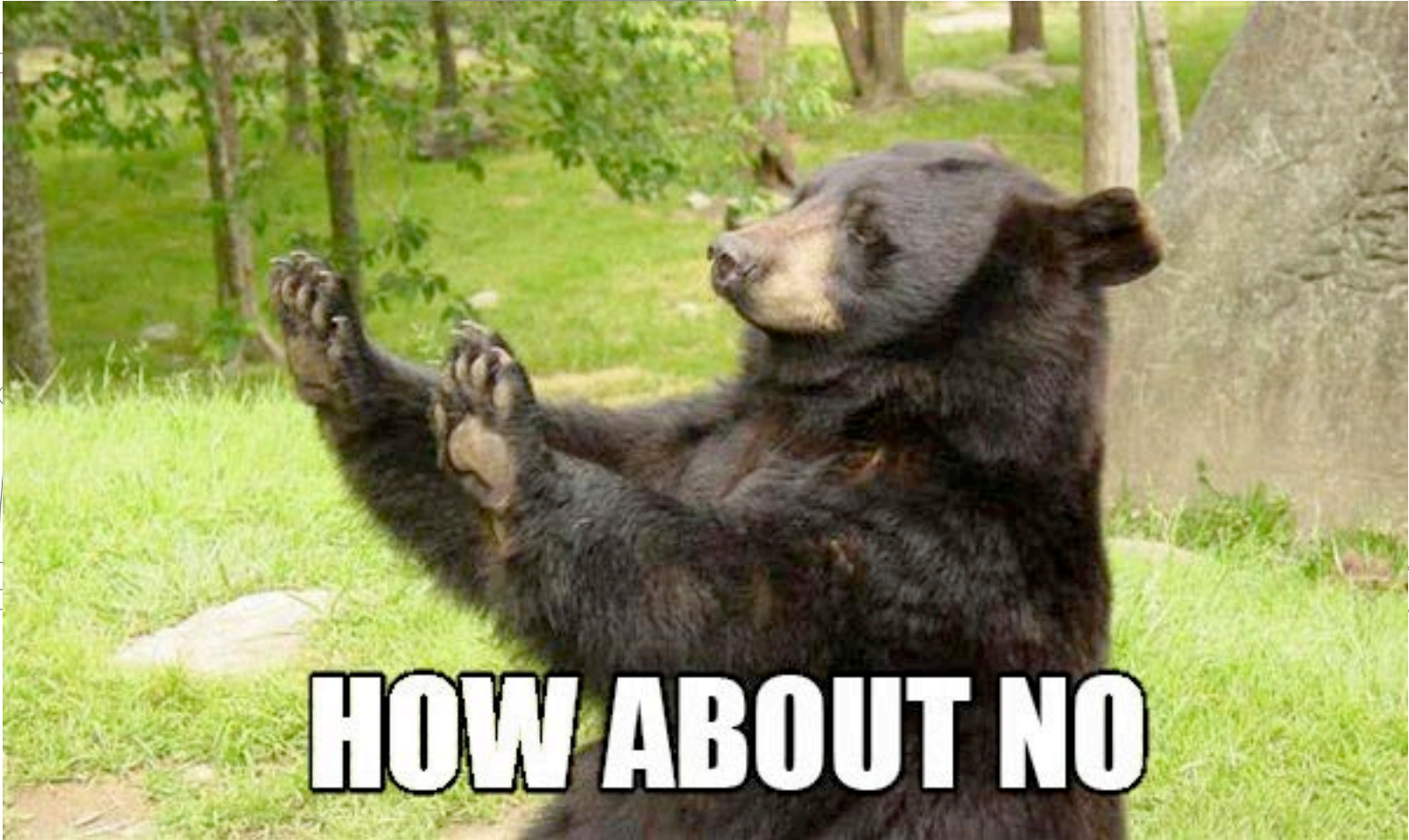


# Multivendor, researcher, coordinator, miscreant





# Multivendor, researcher, coordinator, miscreant



# Limits of Concurrency Modeling using Petri Nets

It's hard to present this stuff in a way that is understandable once you get so many interactions

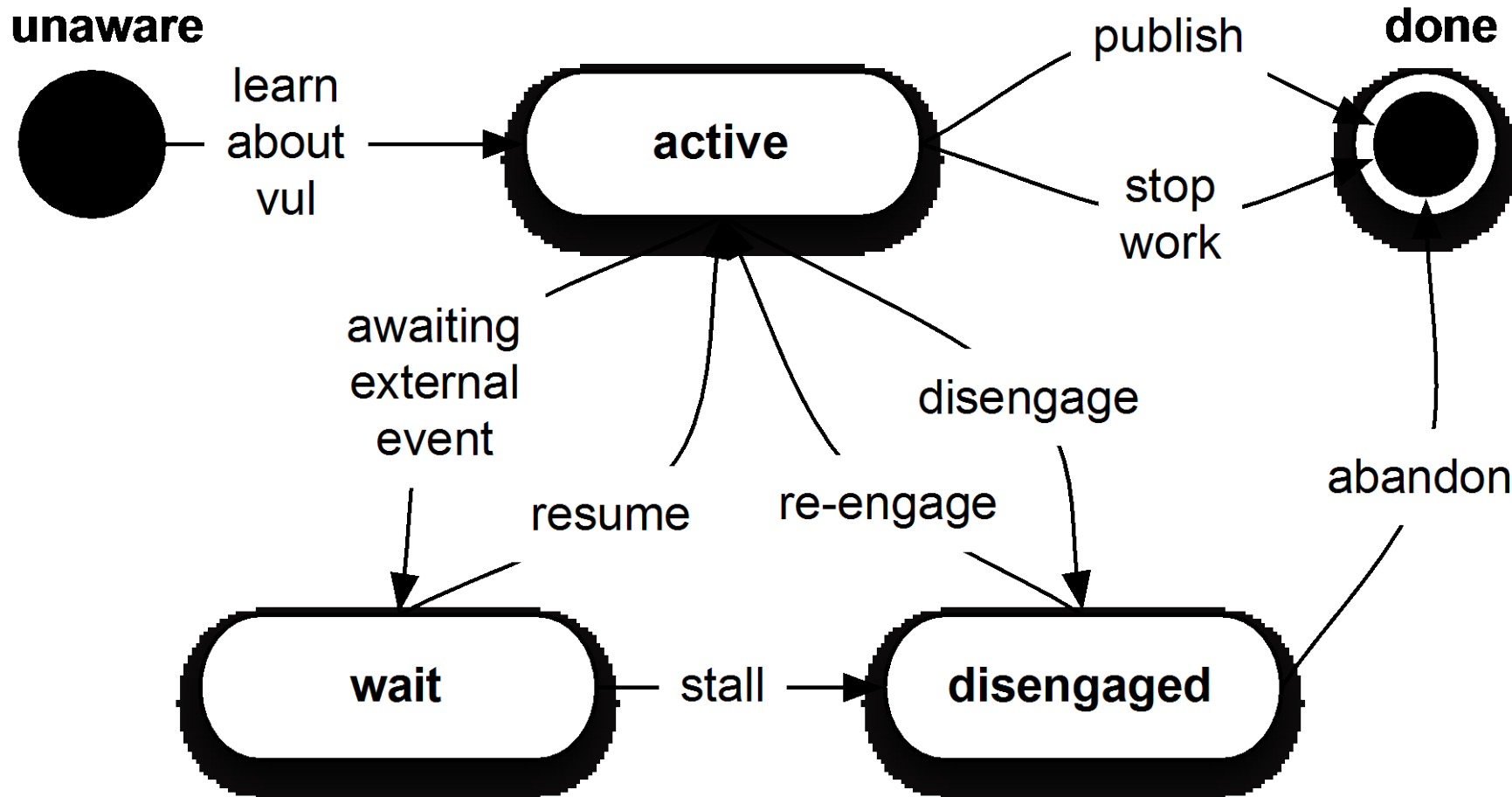
State space grows quickly and the model becomes unwieldy

Hard to model history as it evolves

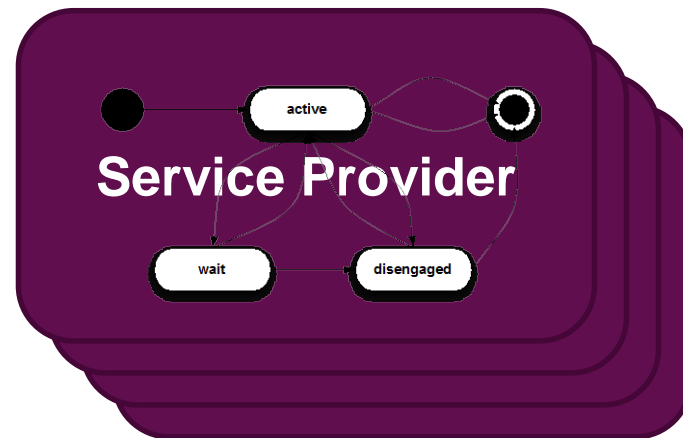
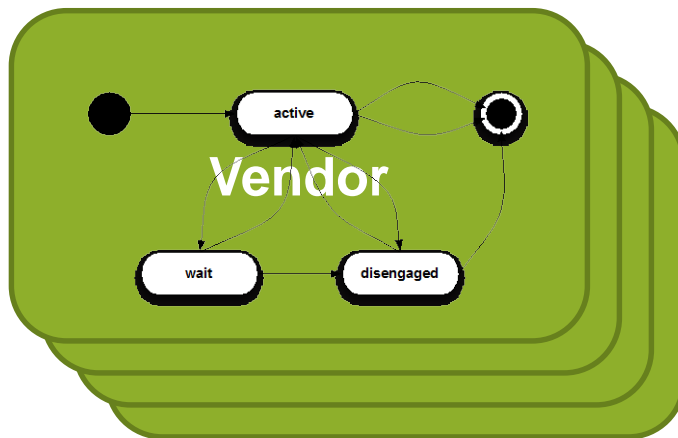
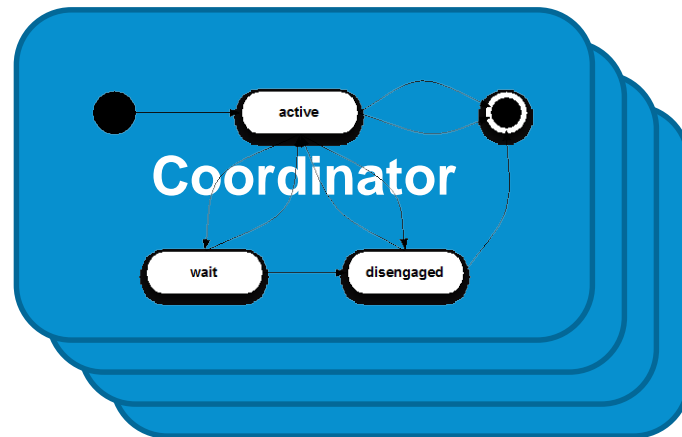
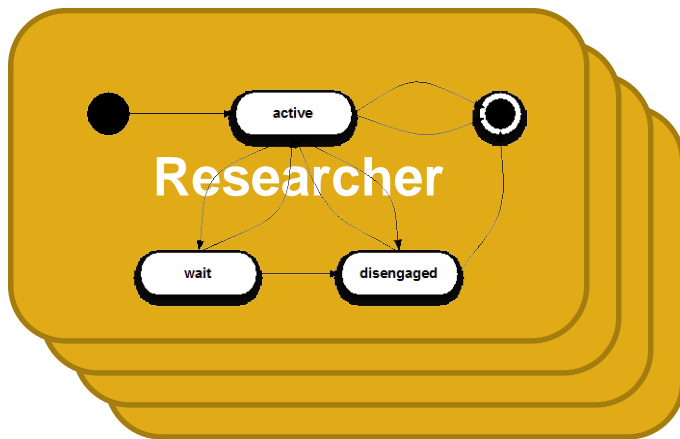
- E.g., when something different happens based on whether you passed through some particular node on the way here

Agent-based models seem promising since they can basically model a state machine per participant and the interactions between them

# Other Ways to Think About It: State Machines



# Modeling Helps You Reason About a Bigger World



What we've learned so far

# Things that break



# Humans

Have

- Knowledge
- Motives (fortune, fame, altruism, challenge, spite, pride, etc.)
- Limited attention
- Emotions
- Biases
- Perceptions
- Expectations

All of these affect decisions and actions

See also Katie Moussouris @ RSA 2013 Flash Talk <https://youtu.be/T6e70upcfI4>

# Researcher / Vendor Communications

## Channel is never established

- Can't find vendor contact
- Contact is nonresponsive

## Receiver saturates / Channel capacity exceeded

- Usually on recipient end
- Human-process / cognitive load

## Channel breaks down

- Synchronization is lost
- Mismatched expectations
- One side goes nonresponsive
- One side goes hostile

## Chilling effects of prior behavior & experience

- See also *iterated prisoner's dilemma strategies*
  - Nice, retaliating, forgiving, non-envious

[https://en.wikipedia.org/wiki/Prisoner's\\_dilemma](https://en.wikipedia.org/wiki/Prisoner's_dilemma)

# One Vendor, Many Vuls

Fuzzing + uniqueness + exploitability analysis = vulplosions

CERT BFF & FOE (fuzzers) highlighted bottlenecks in our own processes and in vendor vul coordination capacity

[msg6333 \(view\)](#)

**Author: reimar**

**Date: 2009-07-03.11:55:02**

On Tue, Jun 30, 2009 at 06:28:54PM +0000, WD wrote:

> Attached is a zip file with multiple (73) files that cause ffmpeg to crash.

A lot of these file crash no longer with SVN, please get rid of those that work now, 73 files are simply too much to handle.





# Many Vendors, One Vul (Type A)

## Heartbleed draws attention to OpenSSL disclosure policy

“The more people you tell in advance the higher the likelihood that a leak will occur. We have seen this happen before, both with OpenSSL and other projects.”

[Maintaining vendor contacts] “is a significant amount of effort per issue that is better spent on other things.”

“We have previously used third parties to handle notification for us including CPNI, oCERT, or CERT/CC, but none were suitable.”

“It's in the best interests of the Internet as a whole to get fixes for OpenSSL security issues out quickly. OpenSSL embargoes should be measured in days and weeks, not months or years.”

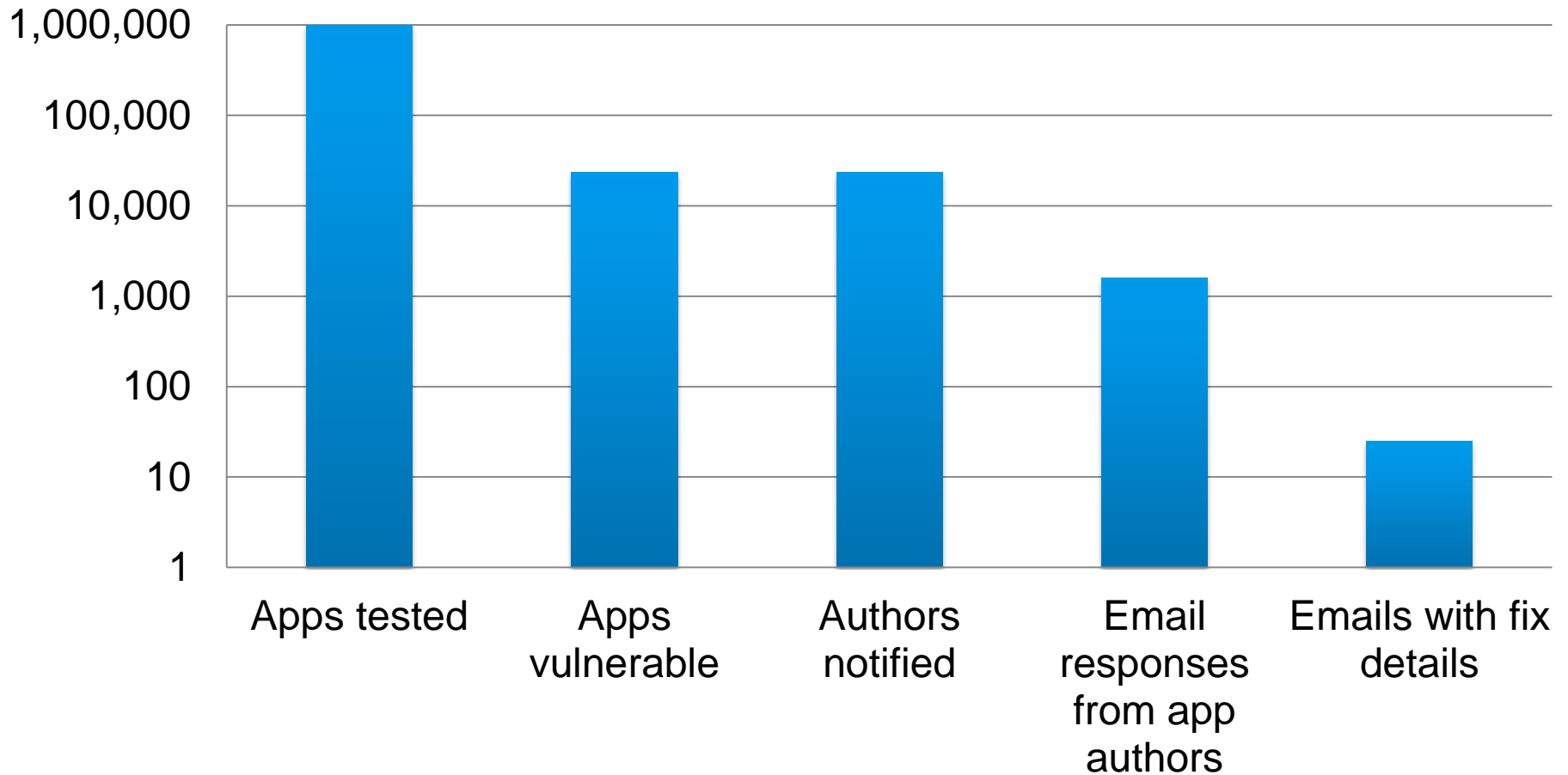
<https://www.openssl.org/about/secpolicy.html>



# Many Vendors, One Vul (Type B)

## CERT Tapioca and the Android SSL MitM avalanche

Find one vul in lots of things, in parallel, as fast as you can



<https://www.rsaconference.com/events/us15/agenda/sessions/1638/how-we-discovered-thousands-of-vulnerable-android>

# Questions We've Asked Ourselves

How do you sustainably notify hundreds of vendors per day for 5 months?

- Use email contact from app store, no attempt at crypto
- Frustrated known vendors because we didn't notify their established security contact

Does the "45 Day Rule" apply to SSL MitM vuls?

- In this case, the attacker doesn't get to pick which apps you use, but you do. (Advantage is to the defender.)
  - Plus, MitM already happening ("Active exploitation" policy clause)
- Originally no advance warning
  - Changed to 7 day advance warning based on vendor feedback

How do you publish 23,000 vulnerability records?

- Used a Google Drive Spreadsheet, our own publishing system couldn't do it easily

# CVE?



**Total apps tested**

**1000462**

**CVE**  
@CVE1

**Total apps that have failed dynamic testing:**

**23667**

We released 5-digit CVE-2014-10001 and 6-digit CVE-2014-100001 IDs on January 13, 2015, plus 90 others. Issues, compliments, or concerns welcome.

📍 Everywhere

🔗 [cve.mitre.org/cve/identifier...](http://cve.mitre.org/cve/identifier...)

 **Tweet to CVE10K**

## Android apps that fail to validate SSL ☆

File Edit View Insert Format Data Tools Add-ons Help View only



Date added			
Temporary filter 2		Range: A1:AA23668	
A	B	P	Q
App	Link	CVE	VU#
Radio 96.1	<a href="http://com.airkast.WBBBFM">com.airkast.WBBBFM</a>	CVE-2014-6025	VU#76993
Clean Internet Browser	<a href="http://com.cleantab.browsee">com.cleantab.browsee</a>	CVE-2014-4905	VU#75075
Brisbane & Queensland Alert	<a href="http://com.queensland.alert">com.queensland.alert</a>	CVE-2014-4906	VU#82528

Watertown Public Library	<a href="http://com.bredir.boopsie.wat">com.bredir.boopsie.wat</a>	CVE PENDING	VU#86260
Schedule Voice Recorder	<a href="http://com.cinix.mobile.record">com.cinix.mobile.record</a>	CVE PENDING	VU#60493
Fun Photo Booth	<a href="http://com.clickpind.fun.came">com.clickpind.fun.came</a>	CVE-2014-6025	VU#66741
REMOVED	<a href="http://com.dev.noifish">com.dev.noifish</a>	CVE PENDING	VU#41476
RVA Homes	<a href="http://com.doapps.android.re">com.doapps.android.re</a>	CVE PENDING	VU#67120
Airbrush Blog App	<a href="http://com.dreamstep.wAirbr">com.dreamstep.wAirbr</a>	CVE PENDING	VU#71185
ONU Mobile	<a href="http://com.dub.app.onu">com.dub.app.onu</a>	CVE PENDING	VU#25003
라바 우리 사는 이야기	<a href="http://com.emj.contentsviewe">com.emj.contentsviewe</a>		VU#99944
Hoarding Photo Frames	<a href="http://com.FavouriteHoarding">com.FavouriteHoarding</a>	CVE PENDING	VU#99380
First Responder	<a href="http://com.firstresponder.ggn">com.firstresponder.ggn</a>	CVE PENDING	VU#20550
穿越宫廷	<a href="http://com.ireadercity.c26">com.ireadercity.c26</a>	CVE PENDING	VU#36478
L'Alsace	<a href="http://com.lalsace_prod.press">com.lalsace_prod.press</a>	CVE-2014-6024	VU#41186
最後意識	<a href="http://com.lastrealized">com.lastrealized</a>	CVE PENDING	VU#10976

# Many Vendors, Many Vuls

## Vulnerability Note VU#317350

ISC DHCP contains a stack buffer overflow vulnerability in handling log lines containing ASCII characters only

CERT® Coordination Center

vulnerabilities, incidents & fixes

security practices & evaluations

survivability research & analysis

training & education

Original Release

Options

Advisories

Vulnerability Notes Database

Incident Notes

Current Activity

### Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

### more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

## CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)

Original release date: February 12, 2002  
Last revised: **Aug 18, 2003**  
Source: CERT/CC

A complete revision history can be found at the end of this file.

### Systems Affected

Products from a very wide variety of vendors may be affected. See [Vendor Information](#) for details from vendors who have provided feedback for this advisory.

In addition to the vendors who provided feedback for this advisory, a list of vendors whom CERT/CC contacted regarding these problems is available from

<http://www.kb.cert.org/vuls/id/854306>

<http://www.kb.cert.org/vuls/id/107186>

**Many other systems making use of SNMP may also be vulnerable but were not specifically tested.**

### Overview

Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. These vulnerabilities may

Intercepting proxy servers may incorrectly rely on HTTP headers to make connections

Original Release date: 23 Feb 2009 | Last revised: 28 Sep 2009

What we've learned so far

# Things that work



# Advice for Vendors

Clear and findable instructions for reporting vulnerabilities

- An email address ([security@example.com](mailto:security@example.com))
- Web forms, bug report systems are okay too
  - if they allow easy marking of security issues

Acknowledge receipt of reports quickly

Set expectations clearly

# Advice for Vendors

Maintain open communication channel with vulnerability reporters

- Occasional “We’re still working on it” notes can keep things from going sideways

Offer a bug bounty

- Be careful to incentivize the right things at the right times

Don’t sue (or threaten to sue) researchers

- Publicity works in counterintuitive ways

Have a “cooperation bias”



# Advice for Researchers

Attempt to contact the vendor before going public

- If you can't find vendor contact or vendor is not responsive, contact a coordinator (like CERT/CC)

Provide clear and concise reports

- Steps to reproduce, proof-of-concept code if possible

If you have constraints, articulate them upfront

- Conference publication deadlines, etc.

Give vendor a final warning before publishing

- Waiting for the vendor is not always possible

# Advice for Researchers

Don't assume the vendor is ignoring you intentionally

- Tickets get closed by mistake
- People change jobs
- Priorities shift
- Errors happen

Know your rights

<https://www.eff.org/issues/coders/vulnerability-reporting-faq>

Have a “cooperation bias”

# Conclusion

# Lies, Damned Lies, and Statistics



Photo: Katie Steiner, 2011

Average stats (like vul reports/year) hide the structure of the vul coordination picture and can mislead you into thinking that the effort involved is trivial.

**It's not.**

You don't build storm sewers to handle your average daily rainfall.

You build capacity for the worst flood you expect over a given timeframe.

And sometimes you'll be wrong.

# There Is No One-Size-Fits-All Disclosure Policy

Traditional shrink-wrapped software

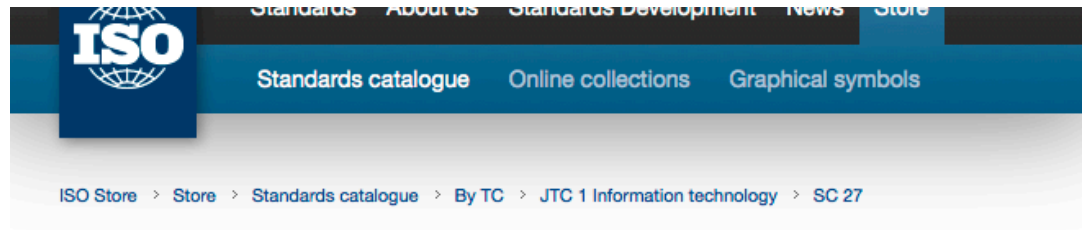
Enterprise customization

Continuous deployment

Mobile apps, App stores

Cloud services (IaaS, PaaS, SaaS)

Embedded devices and smart things



## ISO/IEC 29147:2014

Information technology -- Security techniques -- Vulnerability disclosure

### Abstract

[Preview ISO/IEC 29147:2014](#)

ISO/IEC 29147:2014 gives guidelines for the disclosure of potential vulnerabilities in products and online services. It details the methods a vendor should use to address issues related to vulnerability disclosure. ISO/IEC 29147:2014

1. provides guidelines for vendors on how to receive information about potential vulnerabilities in their products or online services,
2. provides guidelines for vendors on how to disseminate resolution information about vulnerabilities in their products or online services,
3. provides the information items that should be produced through the implementation of a vendor's vulnerability disclosure process, and
4. provides examples of content that should be included in the information items.

ISO/IEC 29147:2014 is applicable to vendors who respond to external reports of vulnerabilities in their products or online services.

## If you have a vulnerability, if no one else can help...

Multiple vendors needed to fix

- Internet Infrastructure
- Third-party libraries

Bug bounties may not apply

- The vendor doesn't offer one
- The terms are unacceptable (or payouts are lame)
- You're otherwise ineligible

Vendor problems

- Non-responsive vendors
- Hostile vendors
  - or fear thereof

Desire to remain anonymous

- Either during disclosure process or long-term

# ...and you can find them...



## Vulnerability Reporting Form



Software Engineering Institute

Carnegie Mellon University

### How to report a vulnerability

We accept reports of security vulnerabilities and serve as a coordinating body that works with

affected vendors. By default, we will share your name with vendors and publicly acknowledge you in documents we publish. If you do not want us to share your name or publicly acknowledge you, select the appropriate responses in the form.

If you are unable to reach the vendor, do not wish for the vendor to know who you are, disagree

with the vendor, please complete the following form. As our [vulnerability disclosure policy](#) explains, we send information submitted in vulnerability reports to affected vendors. By default, we will share your name with vendors and publicly acknowledge you in documents we publish. If you do not want us to share your name or publicly acknowledge you, select the appropriate responses in the form.

Note that we do not coordinate or publish every report we receive. Before submitting this report, please make a reasonable attempt to contact the affected vendor. If you are unable to reach the vendor, do not wish for the vendor to know who you are, disagree

Note that we do not coordinate or publish every report we receive. Before submitting this report, please make a reasonable attempt to contact the affected vendor. If you are unable to reach the vendor, do not wish for the vendor to know who you are, disagree

### Your Contact Information

Provide contact information about yourself in case we have additional questions regarding this vulnerability report. This information is not required to report a vulnerability, but without it we will be unable to contact you.

Name:

Organization:

<https://forms.cert.org/VulReport>

May we [provide your name](#) to the vendor?  Yes  No

Do you want to be [publicly acknowledged](#)?  Yes  No

### Vulnerability Description

Please describe the vulnerability. You can also report multiple vulnerabilities by listing them here.

This field is required.

...maybe you can coordinate with



---

**Software Engineering Institute**  
Carnegie Mellon University®



# For more information

<https://www.eff.org/issues/coders/vulnerability-reporting-faq>

<http://blog.osvdb.org/2013/08/07/buying-into-the-bias-why-vulnerability-statistics-suck/>

<https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm>

<https://www.cert.org/blogs/certcc/post.cfm?EntryID=202>

ISO/IEC 29147 Information technology -- Security techniques --  
Vulnerability disclosure [Externally focused]

ISO/IEC 30111 Information technology -- Security techniques --  
Vulnerability handling processes [Internally focused]

# Contact me

Allen D. Householder

Email: adh at cert dot org

Twitter: @\_\_adh\_\_