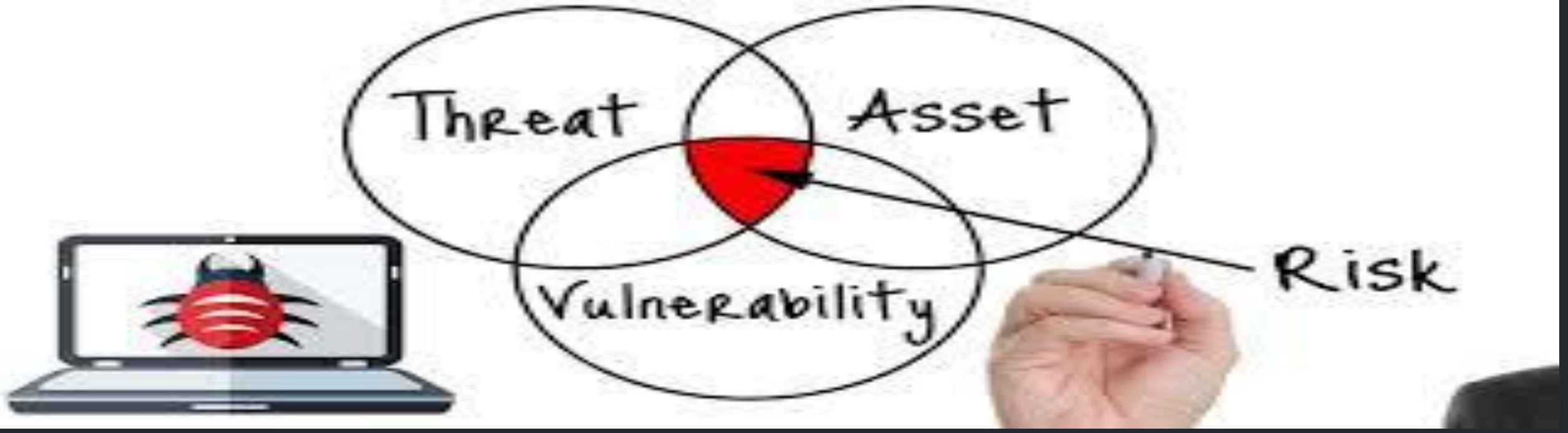
Hey, I found a vulnerability – now what?

the art of sharing what you've found

Hello there!

Lisa Bradley, NVIDIA

CRob, Red Hat



Step 1	Step B	Next Stage	Final Phase
What the heck did I find?	Who the heck do I talk to about this?	How do I tell people about it?	Making !t happen

AGENDA

Step 1

What the heck did I find?

Is it worth telling someone about?

What are you looking at?

- Is it a supported version?
- Is it the latest version?
- Is it a Product or website?
- Is it a 3rd party component?

Can you reproduce it?

Have you looked to see if anyone else has reported this?

- Is it something they probably know about?
- Check public defect trackers/project logs

Don’t dump a fuzzing report!! Do your homework.

1.5)

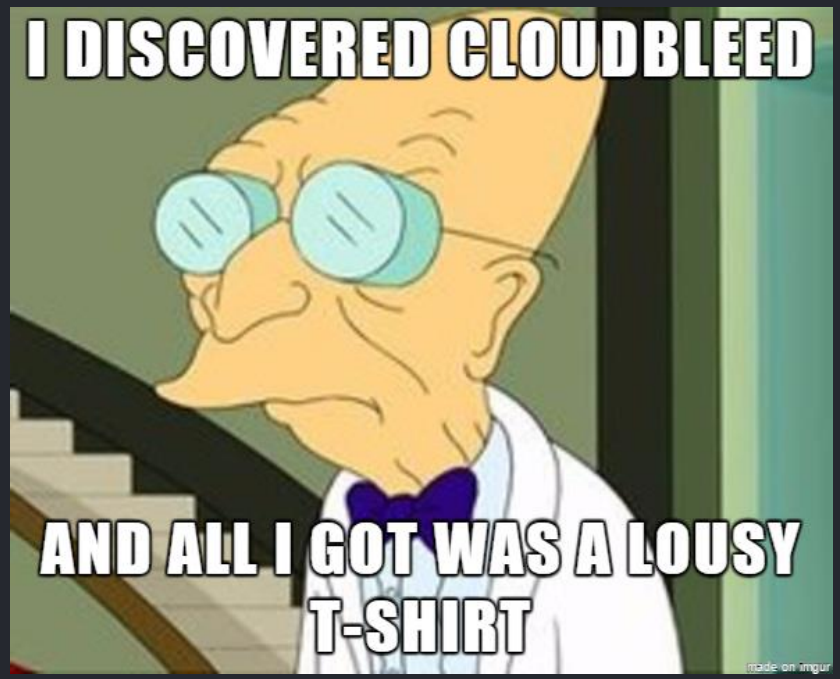
What is your end goal?

The ups and downs of your end goal – are you there to help protect yourself and other consumers, protect the affected party, or go for fame – or can you do it all?

What is your “Why”?

- $$
- Fame
- Helping the most customers
- Conference/Academic Paper
- Future employment opportunities

Each has its own approach and outcome



Step B

Who the heck do I talk to about this?

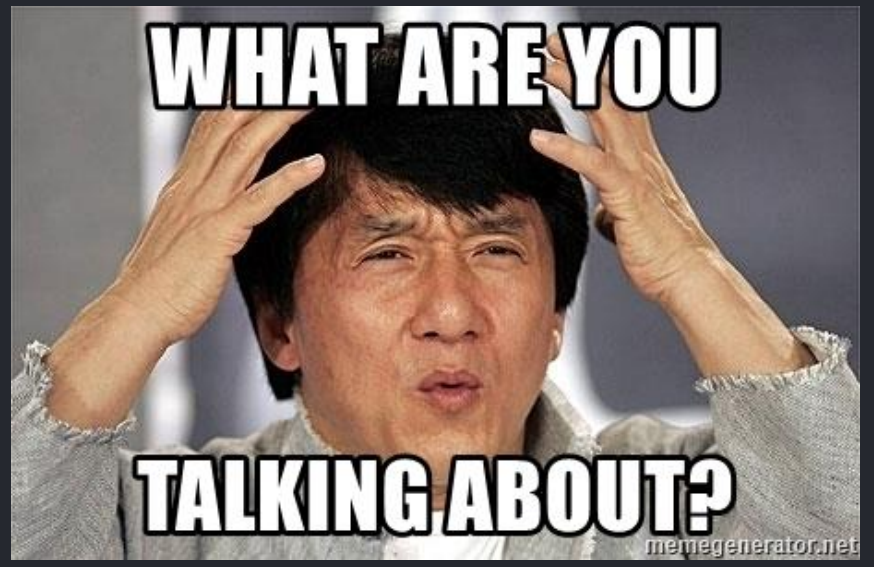
Tell the affected party or maintainer who owns the affected Product/ Package/ Component

Involving the RIGHT people to solve the problem

- Look for the affected party's security website
  - e.g. - *company.com/security or product-security*
  - Attempt to contact affected party directly
    - NO Twitter/public media
- Bug bounty program? -- Hackerone, Bugcrowd etc.
- Don't feel like dealing or can't find out how to -- CERT

What if issue affects more than one company

- Is issue part of a stack? Which product has the issue?
- Who else uses this component?



02.1

Coordinated Vulnerability Disclosure

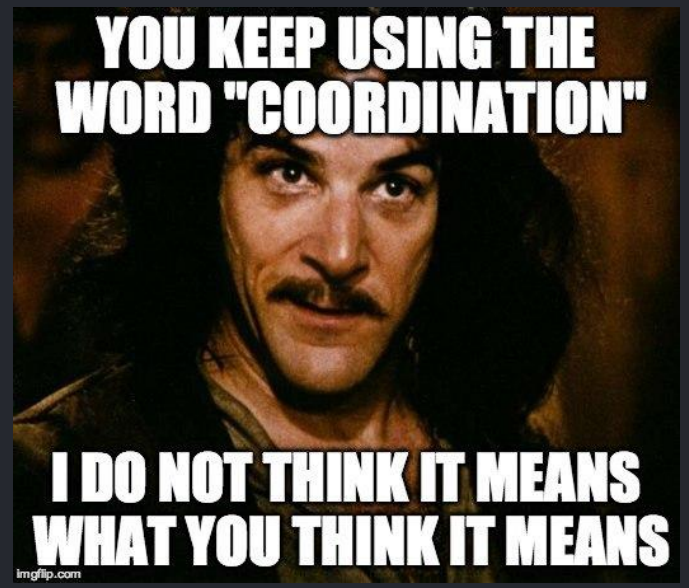
Affected parties share embargoed details about the issue, investigate, and remediate before public disclosure

CVD allows affected party to

- protect customers
- update reporter throughout investigation
- coordinate public disclosures
- appropriately acknowledge reporter

AFTER public remediation released by affected party THEN reporter can publicly discuss issue

This helps ensure that ALL impacted users have access to data and treatment at the same time



Next Stage

How do I tell people about it?

What would you want to know?

Things to think about when disclosing

- Does affected party list what they want to know?
- Do they have a submission form?
- Can data be shared privately - PGP?

- Timeline - Conference/Publication
  - Should you provide a disclosure date?
  - Does the Conference pre-publish your presentation/abstract

ARE YOU FLEXIBLE?

III)

What makes a good vuln. report?

Do you REALLY want to answer 5 million questions? The more you provide up front, the less back-and-forth you'll see

AWESOME TITLE!
==========
Researcher: YOUR NAME or L33T h@x0rr handle!

Contact information: How do you want to communicate about this?

Description
Short, yet descriptive overview of what you've found

Exploitation technique
Local, Remote, other?

Impact(s)
What breaks with the thing you found?

Proof of Concept
POC Code and/or steps to reproduce (can attach a file)

Mitigation
Any suggestions on how to fix it?

Affected versions
What Product, OS, stack and versions have you tested against?

Timeline
Have you shared with anyone else yet (who and when)? Do YOU have a deadline they should be aware of?

Credits
Who should get credit for all of this good work?

d.)

What goes on behind the scenes?

Here is what “the man behind the curtain” is doing

Triage & Analysis

- Reproduce
- Determine priority (severity)
- What other products/versions are affected (scope)
- Testing intense? - regression
- Downstream & Partner/OEM coordination

Things going through affected party’s head

- When is the next release (schedule)?
- How long will this take to fix?
- Crap! Reporter provided a disclosure date!
- Crap! We just released a new version last week!
- Crap we are in a code freeze right now!
- Can we negotiate a new date?

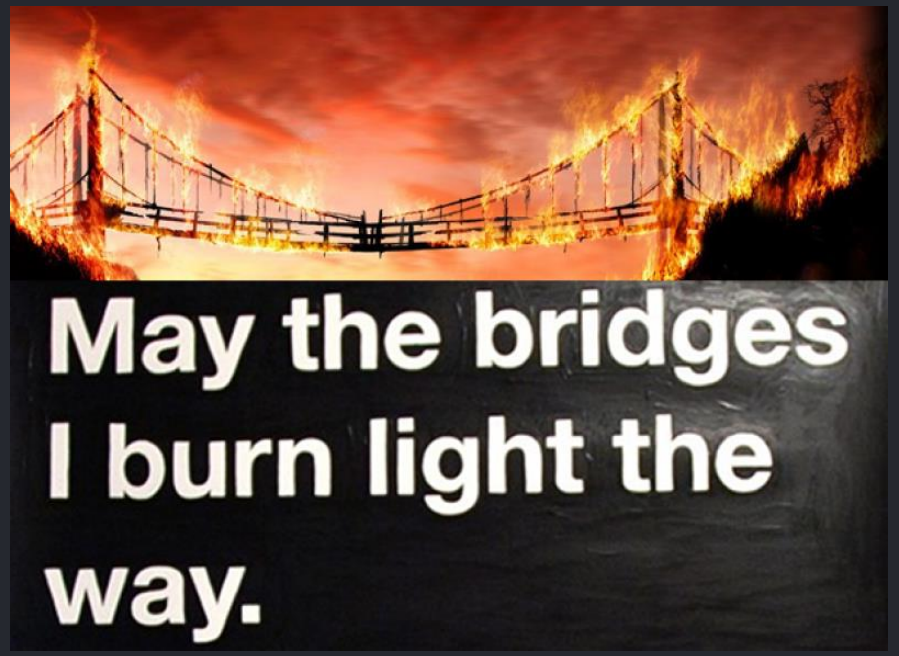
Final Phase

Making !t happen

Now you are going live

How do you want the Public to know about your discovery?

- Brand your bug, or not? CVE?
  - *Be careful...if you brand something the internet thinks you shouldn't be prepared for blowback [e.g. Badlock aka "Sadlock"]*
- Blogging for fun (and profit)
- Provide preview of content to affected party
- Do you talk to Media?
- What was your end goal again? -- future employment opportunities?
- WAIT for the affected party's formal disclosure/security bulletin



Annex

What if?

Patience is a virtue

What if the affected party…

- Does not agree (“it’s a feature, not a bug”)
- Cannot reproduce
- Does not agree with the severity
- Does not assign a CVE

What happens if someone else discovered and disclosed the issue while you were working with the affected party

- What choices you have?

Parting Thoughts....

Be patient; we're all in this together!
Don't be afraid to ask questions
Assume positive intent - We're not all EVIL CORP
Try to be the white hat
Depending on the size of the group you're working with...YOU may be the expert

Thanks for your time!