

RAIN FOREST PUPPY



ETHICS OF SECURITY DISCLOSURE

Intro question recap

- Why do you want the exploit?
- Are you going to do anything bad with the exploit?
- Are you going to tell anyone else about the vulnerability?
- Do you think it's a good idea to pass out the exploit?
- Do you think the public (and bad guys) should have access to the exploit?
- Am I responsible if someone does something bad with the exploit?
- Do you think I should be telling the vendors first?
- Do you think handing out the exploit is in the best interests of those that are vulnerable?



Purpose of disclosure

To get the vulnerability fixed!

Ideal goals of disclosure

- Get the fixes/patches to the 'good guys'
- Give the 'good guys' time to apply the fixes
- All while not alerting the 'bad guys' to the problem

The million dollar question

What is the most appropriate course of action upon discovering a security vulnerability that will maximize safety, minimize damage, and stay within the best interests of the end users?

Personal reasons for disclosure

- "Make the world a safer place"
- Personal agenda
- Political statement
- Love/loathe of involved parties
- Reputation/expertise establishment
- Marketing/PR

These are affected by: age, intent, legality, politics, sociological norms

How much info to disclose...

- Vague placeholder?
- High level report?
- Detailed/technical explanation?
- Working proof of concept confirmation program?
- Working proof of concept exploit program?

Who to disclose it to...

- Immediately forget about it?
- Tell friends? Co-workers?
- Run around and exploit it?
- Alert the vendor?
- Alert the security industry?
- Alert the public/media?
- Alert the bad guys only?
- Alert the good guys only?



Action: forget about it

Pros:

- No hassles!

Cons:

- You (and the rest of the world) remain vulnerable
- Someone else can find problem and use it for evil

Action: tell friends

Pros:

- Friends think your cool 😊

Cons:

- Will one of them use it for evil?
- Secrets are no longer secrets when you tell someone...

Action: use the exploit

Pros:

- Get to drive in FBI squad car and wear shiny handcuffs

Cons:

- See Pros...

Action: tell the vendor

Pros:

- They are the only ones who can officially fix the problem
- They can use their normal resources to alert users of the problem

Cons:

- Vendor doesn't care
- Vendor threatens a lawsuit for reverse engineering
- Vendor strings you along, promising a fix but never delivering
- Vendor takes too long to make a fix
- Open source 'vendors' may have no private forum for disclosure
- Vendor's solution is to purchase the newer version

Action: alert security industry

Pros:

- Provides a 'level playing field'

Cons:

- Bad guys will see it at the same time the good guys do
- General end users don't monitor security-related forums
- Good guys may not react until there is an official resolution

Action: alert public/media

Pros:

- Reaches more of the end users

Cons:

- When has the media ever accurately reported anything technical?
- Severity tends to get intertwined with hype and FUD
- Generally considered to be slimy by industry professionals
- End users/good guys still turn to vendor for official resolution

Action: alert good guys only

Pros:

- Give the people who need to patch time before letting the bad guys know about the vulnerability

Cons:

- Uh....how?

Existing guidelines

- Christey-Wysopal vuln disclosure IETF RFC draft
- CERT/CC policy
- RFPolicy
- Antisec

More resources: <http://www.vulnwatch.org/disclosure.html>

Dilemmas

- Does severity affect the disclosure process?
- What if there is active exploitation 'in the wild'?
- What if the vendor doesn't care, or want to help?
- How does the DMCA and Patriot Act affect disclosure?
- What do you do when multiple vendors are affected?
- What if someone else publicly discloses while you're responsibly working with the vendor?
- What if a patch is not possible?



Current solution

Do whatever you want.

RAIN FOREST PUPPY



ETHICS OF SECURITY DISCLOSURE