Vulnerability disclosure

- Don’t forget overall goal: improve software safety
- Consider incentives for researchers, software vendors, customers
- Supply chain can be complex
  - Software component developers
  - Open source
  - Resellers
  - White-label software

Initial attempts were chaotic

- Researchers would sometimes tell vendors of vulnerabilities
- Vendors would sometimes threaten researchers
- Bugs would sometimes get fixed

Full Disclosure Policy (RFPolicy)

- “This policy states the 'guidelines' that an individual intends to follow. You basically have 5 days (read below for the definitions and semantics of what is considered a 'day') to return contact to the individual, and must keep in contact with them **at least** every 5 days. Failure to do so will discourage them from working with you and encourage them to publicly disclose the security problem.”

Full Disclosure Policy (RFPolicy)

- “First and foremost, a wake-up call to the software maintainer: the researcher has chosen to NOT immediately disclose the problem, but rather make an effort to work with you. This is a choice they did not have to make, and a choice that hopefully you will respect and accept accordingly.”

Full Disclosure Policy (RFPolicy)

- “Compensation is meant to include credit for discovery of the ISSUE, and perhaps in some cases, encouragement from the vendor to continue research, which might include product updates, premier technical subscriptions, etc. Monetary compensation, or any situation that could be misconstrued as extortion, is highly discouraged.”

CERT/CC Vulnerability Disclosure Policy

- “Vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure. Disclosures made by the CERT/CC will include credit to the reporter unless otherwise requested by the reporter. We will apprise any affected vendors of our publication plans and negotiate alternate publication schedules with the affected vendors when required.”

Responsible Vulnerability Disclosure Process (rejected RFC)

- “The Reporter SHOULD grant time extensions to the Vendor if the Vendor is acting in good faith to resolve the vulnerability. “

Microsoft Coordinated Vulnerability Disclosure

- “We ask the security research community to give us an opportunity to correct a vulnerability before publicly disclosing it, as we ourselves do when we discover vulnerabilities in other vendors' products. This serves everyone's best interests by ensuring that customers receive comprehensive, high-quality updates for security vulnerabilities but are not exposed to malicious attacks while the update is being developed. After customers are protected, public discussion of the vulnerability helps the industry at large improve its products.”

Facebook Whitehat

- If you comply with the policies below when reporting a security issue to Facebook, we will not initiate a lawsuit or law enforcement investigation against you in response to your report. We ask that:
  - You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
  - You do not interact with an individual account (which includes modifying or accessing data from the account) if the account owner has not consented to such actions.

Facebook Whitehat

- You make a good faith effort to avoid privacy violations and disruptions to others, including (but not limited to) destruction of data and interruption or degradation of our services.
- You do not exploit a security issue you discover for any reason. (This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues.)
- You do not violate any other applicable laws or regulations.

Facebook refusal

- “Recently, a researcher tried to tell us about a bug that would allow users to post on the timeline of another user who was not their friend. He made headlines when he got frustrated with us and used that vulnerability to post on the wall of a real user.”
- “He tried to report the bug responsibly, and we failed in our communication with him. We get hundreds of submissions a day, and only a tiny percent of those turn out to be legitimate bugs.”
- “We will not change our practice of refusing to pay rewards to researchers who have tested vulnerabilities against real users. It is never acceptable to compromise the security or privacy of other people”

Google Project Zero

- Vulnerability disclosed 90 days after report
- Up to 14-day grace period if patch will be available
- Microsoft has missed two deadlines

> “We believe in coordinated vulnerability disclosure, and we’ve had an ongoing conversation with Google about extending their deadline since the disclosure could potentially put customers at risk. Microsoft has a customer commitment to investigate reported security issues and proactively update impacted devices as soon as possible.” (27 February 2017)

Google Project Zero

- 2016-06-02 - Ian Beer reports "task_t considered harmful issue" to Apple
- 2016-06-30 - Apple requests 60 day disclosure extension.
- 2016-07-12 - Project Zero declines disclosure extension request.
- 2016-07-19 - Meeting with Apple to discuss disclosure timeline.
- 2016-07-21 - Followup meeting with Apple to discuss disclosure timeline.
- 2016-08-10 - Meeting with Apple to discuss proposed fix and disclosure timeline.
- 2016-08-15 - Project Zero confirms publication date will be September 21, Apple acknowledges.
- 2016-08-29 - Meeting with Apple to discuss technical details of (1) "short-term mitigation" that will be shipped within disclosure deadline, and (2) "long-term fix" that will be shipped after the disclosure deadline.
- 2016-09-13 - Apple release the "short-term mitigation" for iOS 10
- 2016-09-13 - Apple requests a restriction on disclosed technical details to only those parts of the issue covered by the short-term mitigation.
- 2016-09-14 - Project Zero confirms that it will disclose full details without restriction.
- 2016-09-16 - Apple repeats request to withhold details from the disclosure, Project Zero confirms it will disclose full details.
- 2016-09-17 - Apple requests that Project Zero delay disclosure until a security update in October.
- 2016-09-18 - Apple's senior leadership contacts Google's senior leadership to request that Project Zero delay disclosure of the task_t issue
- 2016-09-19 - Google grants a 5 week flexible disclosure extension.
- 2016-09-20 - Apple release a "short-term mitigation" for the task_t issue for MacOS 10.12
- 2016-09-21 - Planned publication date passes.
- 2016-10-03 - Apple publicly release long-term fix for the task_t issue in MacOS beta release version 10.12.1 beta 3.
- 2016-10-24 - Apple release MacOS version 10.12.1
- 2016-10-25 - Disclosure date of "task_t considered harmful"

Google Project Zero

- 2016-09-16 - Apple repeats request to withhold details from the disclosure, Project Zero confirms it will disclose full details.
- 2016-09-17 - Apple requests that Project Zero delay disclosure until a security update in October.
- 2016-09-18 - **Apple's senior leadership contacts Google's senior leadership** to request that Project Zero delay disclosure of the task_t issue
- 2016-09-19 - Google grants a **5 week flexible disclosure extension**.

Vulnerability markets

- TippingPoint/ZDI
  - Funded through intrusion detection systems
  - Support disclosure to vendors
- No-rules markets
  - Probably used to develop malware

The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting, Andy Ozment

- “It is thus possible that vulnerability hunting can result in a more secure product and can provide a social benefit. Patch announcements and vulnerability reports are also used to quantitatively (albeit roughly) demonstrate that vulnerabilities are often independently rediscovered within a relatively short time span.”

Heartbleed

- “This bug was **independently discovered** by a team of security engineers (Riku, Antti and Matti) at Codenomicon and Neel Mehta of Google Security, who first reported it to the OpenSSL team. Codenomicon team found heartbleed bug while improving the SafeGuard feature in Codenomicon's Defensics security testing tools and reported this bug to the NCSC-FI for vulnerability coordination and reporting to OpenSSL team.”

Black market

- Unregulated and dubious legality
- Proposals to regulate through munitions control
- Several vendors involved
- Buyers often governments

http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

CIA

- Vulnerabilities unclassified as they are sent to non-US computers
- When should they be reported to vendors?

SHA-1

- Published 1995
- Decertified 2011
- First collision 2017

- “Following Google’s vulnerability disclosure policy, we will wait 90 days before releasing code that allows anyone to create a pair of PDFs that hash to the same SHA-1 sum given two distinct images with some pre-conditions. In order to prevent this attack from active use, we’ve added protections for Gmail and GSuite users that detects our PDF collision technique. Furthermore, we are providing a free detection system to the public.”
- https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html