# Vulnerability Disclosure

## Letting the Cat Out Of the Bag

**Tobias Dussa**
*WP8-T1*

Webinar, July 2021

Public

www.geant.org

# Game Plan

- The general idea of Vulnerability Disclosure.
- Drill-down scenarios:
  - Finding bugs in code,
  - being told about bugs in code,
  - telling people about bugs in code.
- Wrap-up and final musings.
- Questions/discussion/open mike session.

# So Somebody Found a Vulnerability …
# Now What?

# The Bigger Picture

- The general security process calls for the handling of vulnerabilities.
- So how to “handle vulnerabilities”? What are relevant aspects here?

# The Life of a Vulnerability

A vulnerability

- is introduced in some code, then
- is discovered by somebody, then
- is reported to others, then
- is confirmed, then
- is fixed, then
- is published, then
- is eradicated from live systems.

And, of course, it can be *exploited* at any point between the first and the last steps.

# Why “Disclosure”?

- Information about a vulnerability *will* be published in some way, shape, or form sooner or later.
- *Any* player in this game can single-handedly decide to publish whatever information is available, and
- *no* other player can keep others from doing this (technically speaking).

# The Name of the Game

The choice is not *if* to publish information, but *when* and *how* to do so. It is a good idea to minimize the likelyhood of damage. Some efforts to structure the process:

- "Responsible Vulnerability Disclosure Process" (IETF draft),
- "The CERT Guide to Coordinated Vulnerability Disclosure" (CMU/SEI special report).
- ISO/IEC 29147 (ISO standard).

## Commonly-Found Roles

- **Finder**: Discovers a bug.
- **Reporter**: Reports a bug to the vendor.
- Vendor: Owns the software and (hopefully) fixes the bug.
- Deployer: Upgrades the software to a bug-fixed version in the install base.
- **Coordinator**: Does, well, coordination between the different players.

We will discuss the **bold** roles now.

# So You Have {Found, Been Told About, Been Asked to Tell Others About} a Vulnerability

# Finders, Keepers

- Imagine you have discovered a security-relevant bug in some software package.
- Questions to ask yourself:
  - Do I want to report the vulnerability?
  - Who do I want to talk to? Do I have the time and inclination to see this through to the bitter end?
  - What exactly to report?

# “Do I Want to Report?”

- Yes.

# “Who Do I Want to Talk To?” – The Vendor

- Pros:
  - Direct line of communication:
    Minimizes friction losses, maximizes influence.

- Cons:
  - Communication channels possibly hard to establish (points-of-contact potentially unclear, no prior trust relationship, …).
  - All the follow-up woes need to be handled.

# “Who Do I Want to Talk To?” – Some Intermediary

- Pros:
  - Anonymity.
  - Pre-established channels/trust relationships.
  - Follow-up effort offloaded/buffered.
- Cons:
  - Additional layer of indirection.
  - Credit is potentially misassigned.

## “What Do I Want to Report?”

Really depends on the situation.  Some aspects to consider:

- Ultimately, all necessary detail required to assess and fix the vulnerability.
- *However*, depending on the communication channel, not necessarily all at once (establish trust and a secure channel first).
- Minimize noise.

# Additional Considerations

- Be prepared for unresponsive or uncooperative vendors.

  If this is the case, consider introducing external entities as reporter and/or coordinator.
- Be prepared to be responsive and participate in a meaningful and timely manner.

# Becoming a Snitch

- Two potential flavors:
  - Someone in your constituency wants you to proxy a report.
  - Someone wants to report a vulnerability to a vendor within your constituency.
- Fundamental question:
  Are you willing to offer that service?
  - If “Yes”, then excellent.  Go ahead.
  - If “No”, then you should provide pointers to the right point of contact if at all possible.

## Things to Do As a Proxy (i. e., Outbound)

- Do some basic plausibility checks.
- If reporter seeks anonymity: Tread carefully.
- Make sure to give credit where appropriate.
- Be aware of your responsibility.
- In general:
  - Provide sufficiently secure channels of communication.
  - Publish information of how to establish contact.

# Considerations for a Reverse Proxy (i. e., Inbound)

- It is possible (likely?) that the actual vendor could not be reached in a meaningful way, but is in your constituency.

  Therefore, be aware of these possibilities and prepare accordingly:

  - Vendor point of contact hard to find,
  - vendor unresponsive,
  - vendor unwilling to cooperate.
- Also, be prepared to be responsive even if other parties are not.

# Level Up: Coordinating Things

Essentially the same game as being an intermediary (i. e., a reporter), but scaled up (and then some extras):

- Many more parties to talk to,
- many more loose ends to keep track of – in particular, *also* the deploying side,
- greater responsibility – expected to mediate between players.

# Wrap-Up

# Final Remarks

- Coordinated Vulnerability Disclosure is a team effort.
  As always, the name of the game is “be a good neighbor”.
- Be aware that you will very likely be talking to the same parties again some time in the future when the next vulnerability comes around!

## Some More Musings

- It pays off to be prepared, particularly in terms of communication channels.
- Especially coordination efforts can become *very* complex and resource-exhausting → be aware of this possibility and seek help, if in doubt.

GÉANT
Networks • Services • People

# Thank you

Any questions?

www.geant.org


The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).