5.2 Disclosure Choices

As we have mentioned previously, participants in Coordinated Vulnerability Disclosure iterate over the following questions:

1. What actions should I take in response to this knowledge?
2. Who else should I tell about it?
3. What should I tell them?

Let’s take a moment to explore questions 2 and 2a in a few scenarios. Each of these disclosure options have advantages and disadvantages. In this section, we adapt and expand some terminology from Shepherd [1]:

- **No Disclosure** – All information about the vulnerability is kept private. Sometimes this is enforced by non-disclosure agreements (NDAs). Vendors sometimes prefer this scenario to protect trade secrets or to lessen the impact of perceived negative press. Some finders prefer not to disclose vulnerabilities to anyone, in the hope that malicious actors will not find out about the vulnerability if it is not disclosed. Data on the outcomes of a non-disclosure policy are difficult to come by, as these vulnerabilities are by definition hidden from public view.

- **Private Disclosure** – When a product’s vendor is aware of a vulnerability, the vendor may take action to address it but will only notify its own customer base of the vulnerability and its mitigation privately. Many of the same motives as the No Disclosure policy are also in play here; the hope is that malicious actors are much less likely to find out about and exploit a vulnerability if very few people are made aware of the issue. Avoiding negative press is also cited as a reason for this approach. Some vulnerability finders are satisfied by this method if all known customers can be reached, so that everyone using the software may be protected. However, this approach is often not practical for widely deployed or open source software.

- **Limited (Partial) Disclosure** – When a vulnerability is found, only some information about the vulnerability is disclosed to the public. The goal is typically to slow down reverse engineering and exploit development long enough for a fix to be developed and deployed. This is done by withholding proof of concept code or other technical details of the vulnerability while still providing enough information that users of the product may take action to mitigate the issue.

- **Full Disclosure** – When a vulnerability is found, all information about the vulnerability is disclosed to the public. Typically, this scenario results in the release of proof of concept exploit code along with a report describing the vulnerability. In some cases, finders following a full disclosure approach may not attempt to notify the vendor at all in advance of the public release of the vulnerability report. In other cases, they may contact the vendor simultaneously or shortly before issuing a public report. The belief is that this approach serves the greater good by allowing consumers to be aware of the full impact of issues in their products and demand action from vendors, as well as have information available to take appropriate defensive action and make more informed purchasing decisions. Another perceived benefit is that a full disclosure allows other researchers and organizations to reproduce and confirm the vulnerability, whereas a more limited disclosure may not provide enough information to do so. Alternately, this type of disclosure may also be performed by the vendors themselves: many open source projects, for example, handle security issues in the open in order to maximize review of the vulnerability and testing of the proposed solution.

References