What is Vulnerability Coordination?

What is Vulnerability Coordination?

Coordinated Disclosure is the CERT/CC’s preferred terminology for the older “Responsible Disclosure”. Among stakeholders, Coordinated Disclosure is often used to refer to a process where the vendor and the reporter work together to address a vulnerability. The CERT/CC values this approach because it respects the vendor’s desire to prevent the disclosure of vulnerabilities, while still maintaining the right of the reporter to disclose.

A number of philosophies exist regarding the disclosure of software vulnerabilities to the public. A few of them are listed below:

- **No Disclosure** – When a vulnerability is found, all information about the vulnerability is kept private. Sometimes this is enforced by non-disclosure agreements (NDAs). Vendors sometimes prefer this scenario to protect secrets, as well as certain researchers that wish to do the same.

- **Limited Disclosure** – When a vulnerability is found, only some information about the vulnerability is disclosed. 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.

- **Full Disclosure** – When a vulnerability is found by a reporter, all information about the vulnerability including proof of concept should be disclosed immediately. The belief is that this disclosure serves the greater good by allowing consumers to be aware of issues in their products, and demand action from vendors, as well as have information available to make more informed purchasing decisions. Security researchers tend to favor this approach. The vendor is typically not informed prior to disclosure, or at least has a very small window (typically < 1 day) to act. Alternately, this type of disclosure may also be performed by the vendor 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.

- **“Responsible” Disclosure** – When a vulnerability is found by a reporter, the reporter informs the vendor and suggests a timeline for disclosure. The amount of time varies greatly based on the organization. The vendor and reporter typically work together to provide a simultaneous public disclosure after a patch is ready. The disclosure may be Limited Disclosure or Full Disclosure after the timeline has expired. In cases where the vendor and reporter do not agree on a timeline, or the vendor is unresponsive, the reporter may publish anyway at the end of the original proposed timeline. In the CERT/CC’s opinion, the term “responsible” is too vague. The word “responsible” tends to draw focus toward “good” and “bad”, rather than objectively searching for a way to address a problem that was discovered.

- **Coordinated Disclosure** – Coordinated Disclosure is the CERT/CC’s preferred terminology for the older “Responsible Disclosure”. Among others, Microsoft has advocated for coordinated disclosure. Otherwise, Coordinated Disclosure and Responsible Disclosure are the same thing. Often, you will see Coordinated Vulnerability Disclosure abbreviated as CVD.

Another take on this issue is provided at [Wikipedia](https://en.wikipedia.org/wiki/Vulnerability_disclosure).
The CERT/CC believes the Coordinated Disclosure process is the best balance of these competing interests. The public and especially users of the vulnerable component deserve to know issues with their products and how the vendor handles said issues, but at the same time, quickly disclosing such information without review and mitigation only opens the public up to exploit. The best scenario is when everyone can coordinate and work together to protect the public. This coordination can also often be turned into a public relations win for the vendor by quickly addressing the issue.