# What is Vulnerability Coordination?

## What is Vulnerability Coordination?

Coordination is defined by Merriam-Webster as:

> *the process of organizing people or groups so that they work together properly and well*

Vulnerability Coordination is the process by which multiple stakeholders in a software vulnerability work together to analyze and address a vulnerability with the goal of eventually disclosing to the public the existence of the vulnerability and guidance on how to mitigate or fix the vulnerability.

Vulnerabilities are difficult to define, but a vulnerability may be thought of as a flaw in software or hardware components that allows an attacker to perform actions that wouldn't normally be allowed. The impact of such vulnerabilities varies greatly, from being able to learn someone's private email address, to taking control of a computer, to causing physical damage and bodily injury.

The stakeholders vary on a case by case basis, but typically include:

- The reporter of the vulnerability
- The vendor of the component that contains the vulnerability
- Vendors that utilize the component containing the vulnerability in their own products ("downstream vendors")
- The CERT/CC, US-CERT, or other 3rd party organization, if the vulnerability was reported to the 3rd party
- The general public / consumers who purchase products containing the vulnerable component

The CERT/CC's role in coordination is to coordinate these stakeholders, making sure the issue is addressed accordingly and the correct information reaches the public.

## What is Vulnerability Disclosure?

Vulnerability Disclosure is the process by which information about the vulnerability (and advice for mitigating or fixing the vulnerability) are released to consumers of the product, and more generally, the general public at large.

There is no specific way to do this; sometimes, vulnerability information is disclosed in a blog post by the reporter of the vulnerability, or emailed to a security mailing list. Sometimes the vendor issues a security advisory to its customers or to the public. In the CERT/CC's case, we publish Vulnerability Notes on our website, usually in coordination with other simultaneous disclosure methods by the reporter or the vendor.

The amount of information in a disclosure also varies greatly. Some disclosures only warn of a general vulnerability in some specific software; others are more specific and provide actual examples of how to attack the flaw (the examples are called "proof of concept", usually shortened to "PoC").

There is general disagreement on what the "proper" way to disclose a vulnerability is in the security community, as different people and organizations harbor sometimes very strongly differing opinions. As the oldest software vulnerability coordinator in the world, the CERT/CC regularly discusses such issues and opinions with many stakeholders.

## What are the different Vulnerability Disclosure philosophies?

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.

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.