4. Phases of CVD

"You go through phases. You have to reinvent reasons for playing, and one year's answer might not do for another."
-Yo-Yo Ma

There are a number of proposed models of the CVD process that have slightly varying phases [1,2,3,4].

Below, we adapt a version of the ISO/IEC 30111 [5] process with more phases to better describe what we have seen at the CERT/CC:

- **Discovery** – A researcher (not necessarily an academic one) discovers a vulnerability by using one of numerous tools and processes.
- **Reporting** – A researcher submits a vulnerability report to a software or product vendor, or a third-party coordinator if necessary.
- **Validation and Triage** – The analyst validates the report to ensure accuracy before action can be taken and prioritizes reports relative to others.
- **Remediation** – A remediation plan (ideally a software patch, but could also be other mechanisms) is developed and tested.
- **Public Awareness** – The vulnerability and its remediation plan is disclosed to the public.
- **Deployment** – The remediation is applied to deployed systems.

A mapping of CVD phases to CVD roles is provided in Table 2.

Roles Phases	Finder	Reporter	Vendor	Coordinator	Deployer
Discovery	Finds vulnerabilities				
Reporting	Prepares report	Reports vuls to vendor(s) and/or coordinators	Receives reports	Receives reports Acts as reporter proxy	
Validation and Triage			Validates reports received Prioritizes report for response	Validates reports received Prioritizes report for response	
Remediation		Confirms fix	Prepares patches Develops advice, workarounds	Coordinates multiparty response Develops advice, workarounds	
Public Awareness	Publishes report	Publishes report	Publishes report	Publishes report	Receives report
Deployment					Deploys fix or mitigation

Table 2: Mapping CVD Roles to Phases

We will next discuss each of these phases in more detail.

< 3.6. Other Roles and Variations | 4.1 Discovery >

References

1. ISO/IEC, "ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure," 2014.
2. S. Christey and C. Wysopal, "Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt," February 2002. [Online]. Available: https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00. [Accessed 17 May 2017].
3. ISO/IEC, "ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes," 2013.
4. J. T. Chambers and J. W. Thompson, "National Infrastructure Advisory Council Vulnerability Disclosure Framework Final Report and Recommendations by the Council," 13 January 2004. [Online]. Available: https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf. [Accessed 17 May 2017].
5. ISO/IEC, "ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes," 2013.