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.

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

Table 2: Mapping CVD Roles to Phases

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

- 4.1 Discovery
- 4.2 Reporting
- 4.3 Validation and Triage
- 4.4 Remediation
- 4.5 Gaining Public Awareness
- 4.6 Promote Deployment

References