Understanding the Coordination Process

An Overview of the Coordination Process

This process at times involves several organizations.

Ideal Disclosure Process

When working directly with the vendor, generally the coordinated disclosure process proceeds as follows:

1. A security researcher reports a vulnerability to the CERT/CC and requests coordination assistance.
2. CERT/CC analyzes the report, attempting to verify correctness of information, and deciding if it will accept or decline to provide assistance.
3. If the report is accepted by the CERT/CC, then the CERT/CC will attempt to contact the vendor and report the vulnerability.
4. CERT/CC begins planning for public disclosure as a Vulnerability Note after 45 days from initial date of attempted contact, or another date negotiated with the reporter.
5. If the vendor replies, CERT/CC will work with the vendor to develop and test patches if necessary, as well as help notify any downstream vendors affected.
6. If the vendor does not reply, CERT/CC will attempt to alert downstream vendors prior to the disclosure date and then publish the Vulnerability Note after sending a reminder notice to the vendor.
7. Prior to the publication date, a CVE ID is assigned by CERT/CC if necessary (unless the vendor is a CVE Naming Authority, in which case the vendor must assign a CVE ID).
8. The draft Vulnerability Note and CVE ID are shared with the vendor and reporter for comments, typically 1-2 weeks before the publication date. In some scenarios, CERT/CC may decide no to publish, however.
9. On the agreed-upon publication date, public security advisories are published, detailing the issue and how to obtain the patch or mitigate the issues. CERT/CC may publish a Vulnerability Note, and typically the vendor and/or the reporter will also publish their own advisories.

Complications

The above description is very idealized, while every coordinated disclosure case is somewhat unique and may have special handling requirements or constraints. The important idea is the word "coordinated": the formula presented above can be tweaked as much as necessary as long as both parties are kept in the loop (coordinate!).

In some simple cases, should a vendor become unresponsive, some reporters will proceed to publishing a security advisory. This is common, especially in cases where the vulnerability was initially established but then no date is set for a patch release. This is fine to do, but CERT/CC recommends to first reach out to the vendor with a draft of your advisory before publishing.

However, other cases can be more complex, such as reports that affect multiple vendors, only some of which are responsive to the reporter. In general, the CERT/CC is here to help with scenarios that go "off the rails". This can include many different reasons, such as:

- Reporter is new to coordination and disclosure and would like some guidance on reporting and disclosing vulnerabilities
- Vendor is new to coordination and disclosure; the vendor may be unreachable by the reporter, or the vendor may request guidance on handling the report and establishing operations for future reports
- Multiple vendors are suspected of being affected, and the reporter either has received no reply or is even unsure exactly who is affected
- Vendor and Reporter disagree on the existence or severity of a vulnerability; CERT/CC may be able to provide independent testing and analysis

In these cases you can contact the CERT/CC for assistance by using our Vulnerability Reporting Form.

Coordinating via CERT/CC

The best way to submit a report to the CERT/CC is via our Vulnerability Reporting Form.

When working with the CERT/CC, the process is typically very similar but with a few extra steps:

1. Security researcher reports a vulnerability to the CERT/CC and requests coordination assistance.
2. CERT/CC analyzes the report, attempting to verify correctness of information, and deciding if it will accept or decline to provide assistance.
3. If the report is accepted by the CERT/CC, then the CERT/CC will attempt to contact the vendor and report the vulnerability.
4. CERT/CC begins planning for public disclosure as a Vulnerability Note after 45 days from initial date of attempted contact, or another date negotiated with the reporter.
5. If the vendor replies, CERT/CC will work with the vendor to develop and test patches if necessary, as well as help notify any downstream vendors affected.
6. If the vendor does not reply, CERT/CC will attempt to alert downstream vendors prior to the disclosure date and then publish the Vulnerability Note after sending a reminder notice to the vendor.
7. Prior to the publication date, a CVE ID is assigned by CERT/CC if necessary (unless the vendor is a CVE Naming Authority, in which case the vendor must assign a CVE ID).
8. The draft Vulnerability Note and CVE ID are shared with the vendor and reporter for comments, typically 1-2 weeks before the publication date. In some scenarios, CERT/CC may decide not to publish, however.
9. On the agreed-upon publication date, public security advisories are published, detailing the issue and how to obtain the patch or mitigate the issues. CERT/CC may publish a Vulnerability Note, and typically the vendor and/or the reporter will also publish their own advisories.
Please note that when a vulnerability is reported to the CERT/CC, we will begin to manage the process and timeline. We will take reporter's comments into our decision process, but by submitting a report, the reporter agrees that CERT/CC has final decision authority over any coordination and publishing on the CERT.ORG website, and agree to follow our Disclosure Policy by default. However, as the vulnerability reporter, you are the owner of the vulnerability information and are free to disclose it on your own at any time, if you wish.

Per our disclosure policy, we also reserve the right to change this process as necessary. As stated earlier, every case is somewhat unique and may require significant changes to the process depending on the information available.