4.5 Gaining Public Awareness

For defenders, deploying patches requires effort and is often avoided unless there is sufficient justification. Therefore it is important to provide at least a brief description of the vulnerability in the release notes for the updated code. Knowledge of the existence of a vulnerability is often the key driver causing patches to be deployed. A silent fix Where the vendor knows about and fixes the vulnerability but fails to mention the vulnerability’s existence in the subsequent release notes accompanying the new version, is far less likely to be widely deployed than one that is clearly described.

Even within the CVD process, there are still many decisions to be made about the disclosure process. The audience, timing, and amount of information released can vary because of a number of factors. These choices might even vary from report to report, depending on the impact and consequences of a particular vulnerability.

Generally, finders, reporters, vendors, and coordinators should consider the following questions in establishing their policies and practices:

- **Should you disclose at all?** – Generally, the answer will be yes, but there may be factors that influence this decision. For example, some vulnerabilities, if exploited, could place lives in danger or cause severe socioeconomic harm. As a result, it may be prudent for reports of such vulnerabilities to be held indefinitely until the population of vulnerable systems has been reduced through patching or obsolescence. However, any decision to defer disclosure should be considered provisional or contingent on the continued absence of evidence of exploitation or adversarial knowledge of the vulnerability.
- **What information will you disclose?** – For example, will you publish all information about the vulnerability, including proof of concept code, or will you only release a brief description of the problem and a remediation? Generally speaking, there is a minimum amount of information required in order for a vulnerability report to be useful. Recall that the point of disclosure is to provoke some action, most often by developers or other downstream vendors who were not already involved in the coordination process. If the details provided to the recipient are insufficient to cause that action to be taken, the disclosure process will not succeed.
- **To whom will you disclose?** – In most cases, the disclosure should be made publicly. However, in some scenarios the disclosure may be to a specific limited group. For example, if the pool of users is small and the vendor reaches out to every impacted user, a public disclosure may be unnecessary.
- **Via what channel(s) will you disclose?** – Will the vulnerability information be published on the vendor’s website? The reporter’s blog? BugTraq [1], Full Disclosure [2], or other mailing lists? Will you draw attention to it on social media? There are pros and cons to most of these options that must be weighed. When available, an organization’s communications or public relations groups should be involved in planning for the disclosure process.
- **What is your expectation of others in disclosing further (or not)?** – Be sure to discuss your expectations with all stakeholders and be prepared to negotiate.

Vendors in particular will need to address three main questions in providing vulnerability and fix information to defenders:

- What information should be provided about the vulnerability?
- Where should this information be provided?
- What, if any, additional measures should be taken to draw attention to the existence of the vulnerability or the availability of its fix?

**Prepare and Circulate a Draft**

Prior to public announcement of a vulnerability document, we find it helpful to circulate a draft document describing the vulnerability to give CVD participants an opportunity for discussion and commentary.

At a minimum, a draft advisory should be shared between the reporter and vendor to reduce the likelihood of either party being taken by surprise. Ideally, both parties should use this document to coordinate how much information is being released, and what future expectations might exist. Both parties also have the opportunity to correct erroneous information, as well as verify that credit for discovering or reporting the vulnerability is given to the correct person or organization. If multiple vendors are affected, or there are affected downstream vendors making use of the vulnerable software, it can be useful to share a draft with some or all of the affected vendors for even more feedback. Be sure to also discuss what channels to use for publication and disclosure.

The Traffic Light Protocol (TLP) may be useful when sharing draft information. We discuss applications of TLP to CVD in Appendix B.

An example of a template for a vulnerability disclosure document is provided in the appendices.

**When to Engage a Coordinator**

In multiparty CVD, private notifications to other vendors and even public disclosures by individual vendors may not sufficiently raise awareness or accurately reflect the scope of a vulnerability. Because of the role they play in conveying information to a broad audience of system deployers, trusted third parties (non-vendors) such as DHS CISA, the CERT/CC, or other coordinators can help notify affected vendors, facilitate technical analysis of the vulnerability and its impact, and amplify communications to the public. When vendors provide advance notice of major vulnerabilities to the coordinator community, it allows the various coordinating organizations to prepare accurate remediation instructions for system deployers, and to publish that information in synchronization with the vendors’ release of the patches. When that advance notification does not occur sufficiently early, as in the case of Meltdown and Spectre[5], coordinators may be in a rush to understand the issue while preparing their advisories, leading to erroneous or inadequate advice to their constituencies.

**Publishing**
Once the draft circulation phase is complete, the next step is publishing the vulnerability document to whatever channels have been identified during previous phases.

Some vendors have a specific website that lists all their security advisories to date. Others might email the disclosure to a user mailing list or a security mailing list such as Full Disclosure [2] or BugTraq [1]. Reporters themselves may also choose to disclose by posting the advisory to a mailing list or including it in a personal or company blog. A common goal for reporters in the CVD process is to synchronize their publication with the vendor's response. As a result, near-simultaneous publication occurs quite often.

It is generally courteous for the vendor and reporter to contact each other after disclosure to inform one another that the disclosure went through as planned and provide URLs to the published documents.

Avoid Silent Patches

Many vulnerability reports can be similar, and sometimes a vendor or coordinator might receive multiple reports of similar vulnerabilities at the same time. Sometimes this is due to independent discovery, which we discuss in Section 6.5. Other times it reflects a report traversing multiple paths to arrive at its destination within the CVD process. This is fairly common in cases where a vulnerability affects products from multiple vendors. Using a common identifier improves coordination as it ensures that all coordinating parties can keep track of the issue.

The most common identifier in use today is the CVE ID [3], which is meant as a globally unique identifier for a public vulnerability report. CVE IDs can be obtained from the CVE Project at MITRE or one of several CVE Numbering Authorities (CNAs) established by MITRE—typically the vendors of common software products themselves [4]. Both reporters and vendors can request a CVE ID, but reporters should first check if the vendor they are coordinating with is already a CNA. This identifier should be included in any pre-disclosure shared drafts, so that all parties are aware of the common identifier.

Many system deployers use vulnerability scanning tools to discover systems on their network that need to have patches applied. In turn, many vulnerability scanning tools depend on public vulnerability databases such as NVD. Furthermore, NVD entries are largely dependent on CVE ID assignments. When vendors issue updates without acquiring CVE IDs for the vulnerabilities they address, the patch can go unnoticed by the vulnerability databases, scanning tools, and deployers. Therefore we strongly recommend that vendors acquire as many vulnerability IDs as necessary to clearly indicate which vulnerabilities are fixed by specific patches.

A related issue arises when vendors fail to increment their product version numbers when issuing a fix for one or more vulnerabilities. This makes it much harder for coordinators, vulnerability database providers, vulnerability scanning tool vendors, and deployers to differentiate systems affected by a vulnerability from those that are not.

Where to Publish

Publicly disclosing the existence of a vulnerability and the availability of its fix is usually considered to be the primary goal of the CVD process.

Vendors will often provide vulnerability information:

- On the vendor's public website. Many vendors offer a security-focused section within the support section of their online offerings.
- To a public mailing list or a vendor-specific list

Vendors of bespoke software or products with highly focused customer bases are sometimes reasonably confident that they can reach their affected users directly.

These vendors often publish vulnerability and fix information:

- On a customer-only site
- Via a customer support mailing list
- By individually notifying customers, for example through the technical sales channel

However, even with a well-organized customer contact database, it can be difficult for a vendor to be certain that all relevant decision makers are reached in a timely manner. Hence, we recommend that vendors publish at least basic vulnerability and fix announcements to their public website in addition to whatever direct customer contact communications they provide.

References