1.3. Why Coordinate Vulnerability Disclosures?

Vulnerability disclosures fall between two extremes:

1. Disclose everything you know about a vulnerability to everyone as soon as you know it.
2. Never disclose anything you know about a vulnerability to anyone.

Prior research into vulnerability disclosure practices [1] has shown that neither approach is socially optimal. Thus, we are given to hope that we can improve on these extremes by striking a balance in between. But doing so requires several questions to be answered: how much information should be released? To whom? And when? Do you wait for a patch to be deployed before announcing the vulnerability's existence? Do you wait for the patch to be available but not yet deployed? Is it okay to acknowledge that you know of a vulnerability in a product without providing any other details?

It's also important to consider that not all factors are within control of the parties involved in the disclosure process. Adversaries can discover vulnerabilities and use them to exploit vulnerable systems regardless of your participation in a well-coordinated disclosure process. And yet many vulnerabilities might never be exploited in attacks. So how should we approach the question of potential harm and the questions surrounding risk and reward of vulnerability disclosure?

The CERT/CC believes the Coordinated Vulnerability Disclosure (CVD) process provides a reasonable balance of these competing interests. The public and especially users of vulnerable products deserve to be informed about issues with those products and how the vendor handles those issues. At the same time, disclosing such information without review and mitigation only opens the public up to exploitation. The ideal scenario occurs when everyone coordinates and cooperates to protect the public. This coordination may also be turned into a public relations win for the vendor by quickly addressing the issue, thereby avoiding bad press for being unprepared.

Some vendors express concern about the negative attention brought by having a long list of publicly disclosed vulnerabilities in their products. In our opinion, the number of vulnerabilities found in a vendor's products is less valuable as an indicator of the vendor's security stance than the consistency of its response to vulnerabilities in a comprehensive and timely manner. In the end, the goal of CVD is to help users make more informed decisions about actions they can take to secure their systems.

The Forum of Incident Response and Security Teams (FIRST) [2], which consists of many public and private organizations and companies involved in vulnerability and security incident handling, has established a Vulnerability Coordination Special Interest Group to develop some common CVD best practices and guidelines [3]. While the existence of individual vulnerabilities may be unexpected and surprising, these common practices should help lead to fewer surprises for all stakeholders in the CVD process itself.

Governments and international organizations also recognize the need for coordinated vulnerability disclosure practices. In 2015, the Department of Commerce's National Telecommunications and Information Administration initiated a Multistakeholder Process for Cybersecurity Vulnerabilities [4] to develop a broad, shared understanding of the overlapping interests between security researchers and the vendors and owners of products discovered to be vulnerable, and to establish a consensus about voluntary principles to promote better collaboration. The question of how vulnerabilities can and should be disclosed will be a critical part of the discussion, as will how vendors receive and respond to this information. However, disclosure is only one aspect of successful collaboration.

References