3.5. Coordinator

Complicated or complex CVD cases can often benefit from the help of a coordinator. A coordinator acts as a relay or information broker between other stakeholders. Several types of coordinators with slightly different roles and domains exist. We list a few here.

Computer Security Incident Response Team (CSIRT)

A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client. A CSIRT can be a formalized team or an ad-hoc team. A formalized team performs incident response work as its major job function. An ad-hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises [1].

CSIRT with National Responsibility

CSIRTs with National Responsibility, also known as, National CSIRTs, are designated by a country or economy to have specific responsibilities in cyber protection for the country or economy. A National CSIRT can be inside or outside of government, but must be specifically recognized by the government as having responsibility in the country or economy [2]. In addition to functioning as a clearing house for incident response across government departments and agencies, CSIRTs with National Responsibility often have some degree of responsibility or oversight for coordinating vulnerability response across their nation's critical infrastructure. US-CERT, part of the Department of Homeland Security, has been designated as the national CSIRT for the United States. We maintain a list of National CSIRTS on the CERT website [3].

Product Security Incident Response Team (PSIRT)

Over time, Product Security Incident Response Teams (PSIRTs) have emerged as a specialized form of CSIRT, allowing vendors to focus their response to product security issues. Although not all vendors have dedicated PSIRTs, vulnerability response is sufficiently different from security incident response that larger vendor organizations can usually justify having a distinct function to deal with it. PSIRTs usually provide an interface to the outside world to receive vulnerability reports as well as serving as a central coordinator between internal departments for the organization's vulnerability response for its products. When reporting a vulnerability to a vendor, the reporter will usually be communicating with the vendor's PSIRT. For example, Cisco, Oracle, Intel, Microsoft, Apple, Adobe, and others have established internal PSIRTs. Many PSIRTs participate in the Forum for Incident Response and Security Teams [4].

Security Research Organizations

Organizations that perform security research on other vendors' products in the course of their own business sometimes establish their own coordination capability in order to handle the disclosure process for the vulnerabilities they find. A wide variety of organizations perform this kind of security research, whether for profit or for non-commercial reasons. Some examples include managed security service providers, government agencies, and academic research teams. Some of these organizations are vendors of products or services themselves, and combine their PSIRT's vulnerability response capability with their externally facing coordination capability.

Furthermore, organizations that provide vulnerability management and scanning tools and services are often well-positioned to act as a disclosure coordinator for the vulnerabilities their products detect. This applies especially when those vulnerabilities have not already been disclosed to either the vendor or the public. Alternatively, organizations such as these may choose to partner with another coordinating organization in order to promote transparency and reduce the perception of bias in their vulnerability disclosure process.

Bug Bounties and Commercial Brokers

In recent years, a new class of coordinator has emerged in the form of commercial bug bounty program providers. Many individual vendors have established programs to compensate security researchers for their efforts in discovering vulnerabilities in the vendor's products. Creation of a bug bounty program has been noted as an indicator of maturity in vendors' vulnerability response efforts. In some cases, vendor bug bounty programs are enabled by other companies that provide tools and services to facilitate vulnerability coordination. Companies such as BugCrowd [5], HackerOne [6], Synack [7], and Cobalt [8] offer turnkey solutions for vendors who want to bootstrap their own vulnerability response program.

While bug bounty programs help address the vulnerability coordination needs of individual vendors, there still are vulnerabilities that require larger scale coordination. In particular, multivendor coordination remains a challenge for many organizations. As individual vendors have become more mature in their handling of vulnerabilities in their products, the role of multivendor coordination has increased in importance for more traditional vulnerability coordinators such as the CERT/CC [9], NCSC-NL [10], NCSC-FI [11], and JPCERT/CC [12].

Information Sharing and Analysis Organizations (ISAOs) and Centers (ISACs)

Information Sharing and Analysis Organizations (ISAOs) and Centers (ISACs) are non-government entities that serve various roles in gathering, analyzing, and disseminating critical infrastructure cybersecurity information across private sector organizations of various sizes and capabilities [13,14]. These organizations have only begun to emerge in earnest within the past few years, but they are already actively involved in the coordination and deployment of vulnerability mitigations. Furthermore, it seems likely that some number of critical infrastructure sectors will need to become involved further in the coordination of the vulnerability discovery, disclosure, and remediation processes.

Reasons to Engage a Coordinator

There are a number of reasons that a finder, reporter, or vendor may wish to engage a third-party coordinator to assist with the CVD process.

Reporter Inexperience

Novice reporters sometimes request assistance from coordinators to increase the chances of a successful resolution to the vulnerability they have found. Working with a coordinator for the first few cases can help develop a reporter's knowledge of the CVD process. From the coordinator's perspective, working with novice reporters serves to transfer knowledge of CVD to the security research community, thereby improving vulnerability response overall. We have found that novice reporters usually learn quickly and are willing to do most of the coordination effort themselves, but just need occasional advice on how the process should work.

Reporter Capacity

Seeing a CVD case through to resolution can at times be a protracted process. Not all reporters have the time or resources to follow up on vulnerabilities they've reported. In such situations, a coordinator can help by offloading some of the effort. However, coordinators are often limited in their capacity as well, and must accordingly prioritize the cases they choose to take on. As a result, coordinators and reporters alike should take care to set clear expectations with each other as to what roles they expect to play in any given coordination case.

Multiple Vendors Involved

At its most effective, CVD follows the supply chain affected by the vulnerability. As a mental model, it can be useful to think of the supply chain as horizontal or vertical. A horizontal supply chain implies that many vendors need to independently make changes to their products in order to fix a vulnerability. A vertical supply chain implies that one vendor might originate the fix, but many other vendors may need to update their products after the original fix is available. Software libraries tend to have vertical supply chains. Protocol implementations often have horizontal supply chains.

We discuss horizontal and vertical supply chains in Section 5.4 below.

CVD Disputes

Occasionally vendors and reporters have difficulty arriving at a mutually acceptable response to the existence of a vulnerability.

Disputes can arise for many reasons, including the following:

- Whether the behavior described in the report is reproducible
- Whether the behavior described in the report has security implications
- The impact of the vulnerability to deployed systems
- Whether to publicly disclose the vulnerability
- How much detail to include in a public disclosure
- The timing of public disclosure
- Whether extensions should be made to deadlines set by one party or another, whether or not they have been mutually agreed to previously

In these situations, and many others, reporters and/or vendors may find it useful to engage the services of a third-party coordinator to assist with conflict resolution. Drawing on the experience and relative neutrality of a third-party coordinator can often dissipate some of the potential animosity that can arise in contentious cases.

Major Infrastructure Impacts

In situations where a vulnerability has the potential for major impact to critical infrastructure, it may be necessary to coordinate not only with vendors to fix the vulnerable products, but also with major deployers. The primary concern in these cases is to ensure that internet and other critical infrastructure remains available so that deployers and other network defenders can acquire and deploy the necessary information and patches.

Luckily this scenario is rare, but we have seen it come up in cases affecting internet routing, the Domain Name System (DNS), internet protocols, and the like. Vulnerabilities that affect basic Internet services such as DNS (which also serves as an example of a horizontal supply chain) affect a massive number of vendors; a coordinator can help contact and disseminate information to vendors, service providers, and other critical organizations for quick remediation.

< 3.4. Deployer | 3.6. Other Roles and Variations >

References

1. CERT Division, "CSIRT Frequently Asked Questions (FAQ)," Software Engineering Institute, [Online]. Available: https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm? [Accessed 16 May 2017].
2. CERT Division, "Incident Management: Resources for National CSIRTs," Software Engineering Institute, [Online]. Available: https://www.cert.org/incident-management/national-csirts/index.cfm. [Accessed 16 May 2017].
3. CERT, "List of National CSIRTs," [Online]. Available: https://www.cert.org/incident-management/national-csirts/national-csirts.cfm. [Accessed 23 May 2017].
4. BugCrowd, "BugCrowd," [Online]. Available: https://bugcrowd.com/. [Accessed 23 May 2017].
5. FIRST, "FIRST Teams," [Online]. Available: https://www.first.org/members/teams. [Accessed 16 May 2017].
6. BugCrowd, "BugCrowd," [Online]. Available: https://bugcrowd.com/. [Accessed 23 May 2017].
7. HackerOne, "HackerOne," [Online]. Available: https://www.hackerone.com. [Accessed 23 May 2017].
8. SynAck, "SynAck," [Online]. Available: https://www.synack.com. [Accessed 23 May 2017].
9. Cobalt Labs Inc., "Cobalt," [Online]. Available: https://cobalt.io/. [Accessed 23 May 2017].
10. CERT, "Vulnerability Analysis," [Online]. Available: https://www.cert.org/vulnerability-analysis/. [Accessed 23 May 2017].
11. National Cyber Security Centre Netherlands, "NCSC-NL," [Online]. Available: https://www.ncsc.nl/english. [Accessed 23 May 2017].
12. NCSC-FI, "Finnish Communications Regulatory Authority / National Cyber Security Centre Finland," [Online]. Available: https://www.viestintavirasto.fi/en/cybersecurity.html.
13. JPCERT/CC, "Japan Computer Emergency Response Team Coordination Center," [Online]. Available: https://www.jpcert.or.jp/english/. [Accessed 16 May 2017].
14. U.S. Department of Homeland Security, "Information Sharing and Analysis Organizations (ISAOs)," [Online]. Available: https://www.dhs.gov/isao. [Accessed 23 May 2017].
15. National Council of ISACs, "National Council of ISACs," [Online]. Available: https://www.nationalisacs.org/. [Accessed 23 May 2017].