3.1. Finder

A finder is an "individual or organization that identifies a potential vulnerability in a product or online service," noting that "finders can be researchers, security companies, users, governments, or coordinators." In the interest of consistency, we will use this definition of finder, although in other documentation we've used the term discoverer for this same role. We do, however, distinguish between the role of finder and the role of reporter, as seen in this section and the next.

Vulnerabilities can be found by just about anyone. All it takes is for someone to notice an unexpected or surprising behavior of a system. Although it is common for independent security researchers to hunt vulnerabilities as either a hobby or profession, finders need not self-identify as security researchers or hackers.

Vulnerabilities have been found by people of many backgrounds:

- students and professional academics studying novel ways to exploit systems or protocols
- open source developers who notice that a software bug has security implications
- system administrators who recognize a vulnerability during the course of troubleshooting a system error
- professional security analysts who observe a previously unknown product vulnerability while testing an organization's infrastructure during a penetration test engagement
- people using software or web services who mistyped some input or simply clicked on the wrong thing
- children who like to press buttons. Kristoffer Von Hassel, a five-year-old from San Diego discovered a vulnerability in Microsoft's Xbox Live service just by holding down the space bar and was able to log in to his father's account without the password [1].

There are also organizations that look for vulnerabilities. Some of them work under contract to vendors directly. Some work for the vendors' customers who deploy the software. And some have independent motivation to find vulnerabilities, perhaps to demonstrate their competence in finding vulnerabilities in the interest of their security consulting practice's business development.

Furthermore, vendors may choose to look for vulnerabilities in their own products—a practice that we strongly encourage. This can be done via (a) in-house expertise and testing, (b) contracted security testing, or (c) solicited on a per-vulnerability basis using a bug bounty program. Many vendors integrate testing for vulnerabilities into their development process. Microsoft, for example, includes static, dynamic, and fuzz testing for vulnerabilities in its phases of the Security Development Lifecycle [2]. The BSIMM model suggests that many vendors in various industries already employ techniques in architecture analysis, code review, and security testing to find vulnerabilities as part of their development cycle [3].

Regardless of who finds a vulnerability, there are a few common events that follow the discovery:

1. The finder composes a vulnerability report, as discussed in 4.2 Reporting.
2. The finder (or reporter, if these are distinct individuals) provides that report to someone. Often the vulnerability report would be provided to the vendor, but that’s not always the case. Sometimes the report might be sent to a coordinator. If the vulnerability is discovered internally to a vendor, then the report may simply be forwarded to the responsible team within the organization—for example, filed as a security-related bug report. We cover the coordinator role in Section 3.5. A discussion of the reporting process can be found in 4.2 Reporting.
3. (Optional) Finders, reporters, vendors, or coordinators might prepare a document to publish. The finder often wants to draw attention to his or her discovery and subsequent analysis by publishing a document, blog post, or conference presentation, to share the findings with a larger audience. Vendors typically want to publish a document as well to inform their users that action has been taken to resolve the problem, and to prompt their users to take any required remediation actions. Publishing of vulnerability information is covered in 4.5 Gaining Public Awareness.

It is of course possible for a finder to find a vulnerability and tell no one. However, in that case there is no disclosure involved so we do not address that scenario further in this document.

References