4.3 Validation and Triage

Extraordinary claims require extraordinary evidence.
– Carl Sagan

When a vendor or coordinator receives a vulnerability report, it's usually necessary to prioritize it along with other vulnerability reports already in progress, new feature development, and possibly other non-security bug fixes. As a result, there are a few considerations to be made in dealing with incoming reports.

Validating Reports

Vulnerability reports received from potentially unknown sources may hold inaccurate information. One of the first tasks for the receiver of a report is to analyze the report's validity. A vulnerability report is basically an assertion that some set of conditions exists that permits an adversary to take some action in support of a goal. But just because it was reported doesn't make it true. Replication of the salient claims made in the report is an important step in the case handling process.

Recognizing High-Quality Reports

Not all reports are actionable. Some reports may under-specify the problem, making it difficult or impossible to reproduce. Some may contain irrelevant details. Some will be well written and concise, but many will not. Some reports could describe problems that are already known or for which a fix is already in the pipeline.

In easy cases, a simple description of the vulnerability, a screenshot, or a copy/pasted snippet of code is all that is necessary to validate that a report is likely accurate. In more complex scenarios, stronger evidence and/or more effort might be required to confirm the vulnerability. Responsive vendors should ensure analysts have access to appropriate resources to test and validate bugs, such as virtual machines (VMs), a testing network, and debuggers.

It may be that reproducing the vulnerability is beyond the capability or time available by the first-tier recipient at the vendor. Most often this occurs when the conditions required to exploit the vulnerability are difficult to reproduce in a test environment. In this case, the triager can weigh the reputation of the reporter against the claims being made in the report and the impact if they were to be true. You don't want to dismiss a report of a serious vulnerability just because it is unexpected. A reporter with a high reputation might give weight to an otherwise low-quality report (although in our experience finders and reporters with a high reputation tend to have earned that reputation by submitting high-quality reports).

If there is difficulty in reproducing the vulnerability, follow up with the reporter promptly and courteously; be sure to be specific about what you tried so that the reporter can provide effective advice. In some cases, a report might be placed in a holding pattern while additional information is requested from the reporter.

The possibility also exists that someone could be sending you reports to waste your time, or erroneously believes the report is much more serious than your analysis suggests. Not all reports you receive warrant your attention. It is usually reasonable to decline reports if you provide the reporter with a summary of your analysis and the ability to appeal (presumably by providing the needed clarifying information).

Reporters should review Section 4.2 to ensure the report contains enough details for the recipient to verify and reproduce a vulnerability. Be as specific as you can. Vendors that follow up with questions are doing the right thing, and attempting to validate your report; be friendly and courteous and attempt to provide as much detail and help as you can.

Triage Heuristics

Even for the reports a vendor accepts as legitimate and worthwhile, it is likely that the development team does not have time to address every report at the moment it arrives. Thus, if a report is found to be valid, the next question is how to allocate resources to the report. Most often this requires some measure of how severe the vulnerability is. In some scenarios, the vulnerability may be a critical flaw that requires immediate action, while other cases might indicate a very rare and hard-to-exploit vulnerability that should be given a low priority.

There are a number of heuristics for evaluating the severity of vulnerabilities. Perhaps the most commonly known of these is the Common Vulnerability Scoring System (CVSS) [1]. This system allows a short standard description of the impact of a vulnerability and can be mapped to a score between 1.0 and 10.0 to help prioritization. A related but different metric is the Common Weakness Scoring System (CWSS) [2]. Whereas CVSS addresses the detailed impact of a specific vulnerability, CWSS can be used to evaluate the impact of a class of weaknesses. While scoring systems like CVSS and CWSS can be useful at establishing relative severity among reports, care must be taken in their use since scores do not always map well onto a vendor's or deployer's priorities.

Vendors should ensure their analysts are trained in the chosen heuristic and understand its strengths and weaknesses so that its result can be overridden when necessary. We do not, for example, recommend blind adherence to hard cutoffs such as "We only bother with reports that have a CVSS score greater than 7.0." No vulnerability scoring system is so precise. Ideally, whatever prioritization scheme is used should also be made transparent to reporters so that the process is understood by all stakeholders. Transparency in this part of the process can help prevent frustration and confusion when reporter and vendor disagree on severity of a vulnerability.
References