5.6 Maintaining Pre-Disclosure Secrecy

Three can keep a secret, if two of them are dead.

-Benjamin Franklin

The more people who know a secret, the more likely it is to leak. Simple probability theory tells us that even if the probability of any given party leaking is very low, the cumulative probability of a leak increases exponentially with the number of parties involved [1].

Returning to our simple model, and the "Who needs to know what, when?" question, multiparty disclosure highlights the need to balance need-to-know with need-to-share. There are varying degrees of need-to-know. Not everyone needs to know the same thing at the same time. Patch originators are usually notified early in the process, since their answer to "What do I need to do in response to this knowledge?" (i.e., create a patch) is often on the critical path for any downstream parties to be able to take action. Downstream vendors (patch consumers) and deployers can be notified later.

Coordinating Further Downstream

Vulnerabilities having the potential for significant impact can lead to coordination efforts beyond the traditional product vendor space. Infrastructure and service providers are sometimes brought in early, if there are mitigations that can be deployed in advance of the availability of a fix. This can be especially helpful in cases where the vulnerability may affect the infrastructure necessary to distribute the patch in the first place.

Do You Include Deployers?

Be careful to consider fairness though: By what criteria should you notify service provider X but not service provider Y? At some point, the complexity of who knows what gets high enough that the likelihood of a leak goes to 1, and you might as well go public.

Complex Communications Reduce Trust

It's also important to be aware that not all participants along the chain of disclosure will be equally trustworthy. That's not to say they are actively malicious, just that they may have incompatible values or priorities that lead them to disclose the existence of the vulnerability to others earlier than you'd prefer.

< 5.5 Response Pacing and Synchronization | 5.7 Disclosure Timing >

References

1. D. R. Grimes, "On the Viability of Conspiratorial Beliefs," *PLOS One,* vol. 11, no. 1, p. e0147905, 26 January 2016.