

Zero-Days and Responsible Disclosure: The Window Nobody Can Patch Yet

Fri, Aug 14, 4:00 PM EDT · <https://scottslab.io/posts/zero-days-and-responsible-disclosure>



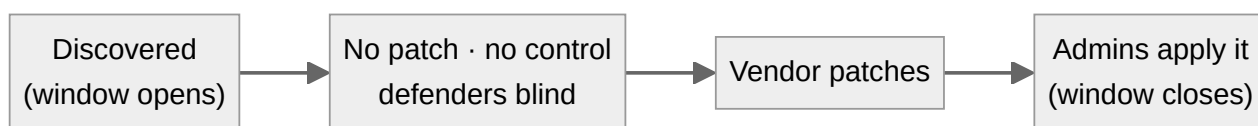
TL;DR

A zero-day is a vulnerability nobody's supposed to know about yet: no patch, no compensating control, defenders blind. The window of vulnerability opens the moment it's discovered and closes only when the vendor ships a fix and admins apply it. A researcher who finds one has three choices: tell the vendor privately, go public, or withhold it (exploit or sell, which is where the ethics end). Responsible disclosure threads the needle: tell the vendor first, set a public deadline, and let the clock create pressure to patch.

"Zero-day" gets used loosely, so pin it down: it's a vulnerability unknown to the people who'd defend against it, with no patch available and no compensating control in place. That's what makes it dangerous: not that the bug is clever, but that nobody's watching for it, so there's nothing standing between it and the systems it affects.

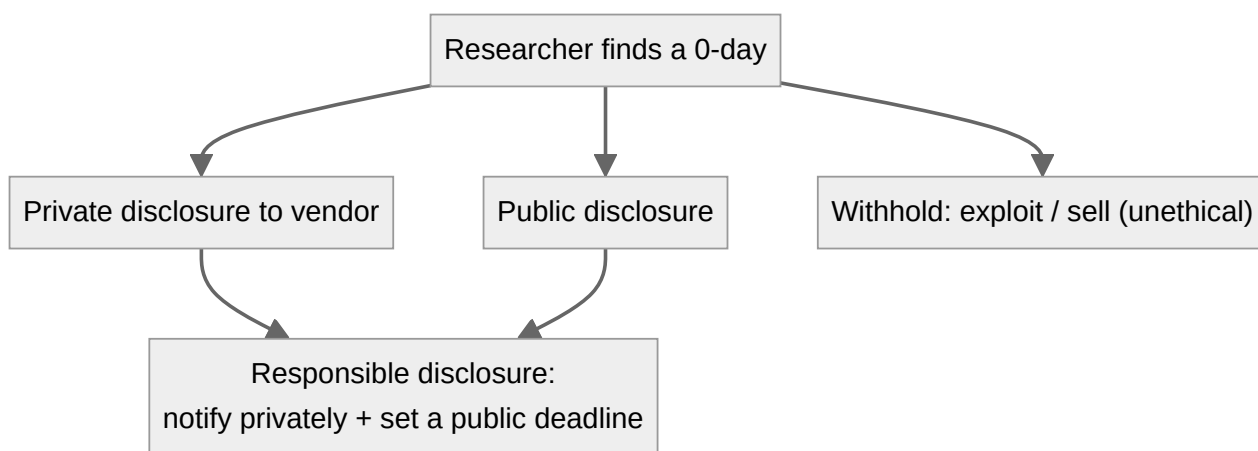
The useful mental model is the window of vulnerability. It opens the instant the flaw is discovered and stays open until two things happen: the vendor releases a patch, and administrators actually apply it. That second half is the one people forget. Once the vendor ships a fix the flaw technically stops being a zero-day and becomes an *n-day* (a known, patchable bug), but an unpatched server is just as exposed to it, and now the patch itself hands attackers a roadmap for building the exploit.

The whole game of disclosure is about closing that window fast without handing attackers a head start while it's open.



Zero-Days and Responsible Disclosure: The Window Nobody Can Patch Yet

A researcher who finds one has three options, and only some are defensible. They can disclose privately to the vendor and let them fix it quietly. They can disclose publicly. That warns everyone, including attackers. Or they can withhold it: sit on it, exploit it themselves, or sell it on the black market. That's unambiguously the unethical path, because it leaves everyone exposed for someone's private gain.



Zero-Days and Responsible Disclosure: The Window Nobody Can Patch Yet

The community standard is responsible disclosure, and it's a deliberate compromise. You notify the vendor privately first, giving them a real chance to fix it before anyone else knows. But you also set a public disclosure deadline: a date you'll go public whether they've patched or not. That deadline is the whole point: private notice alone lets a vendor sit on a fix indefinitely, while immediate public disclosure endangers users. The deadline balances the two: enough time to remediate, enough pressure that they actually do.