This Article argues that intellectual property law stifles critical research on software security vulnerabilities. Researchers who discover flaws often face legal threats based on IP claims if they reveal findings to anyone other than the software's vendor. Externalities and network effects cause vendors' incentives to diverge from those that are socially optimal. Unlike previous scholarship, the Article locates the problem of barriers to security research as one of information's distribution. It proposes a set of key reforms – legal "patches," in software terms – to protect socially valuable research, guide behavior by those searching for vulnerabilities, and channel dissemination of vulnerability data towards legitimate consumers. The Article argues for three types of change: legal, social, and market-based. Legal reform would create immunity from IP liability for researchers who conform their behavior to prescribed rules, which conform roughly to the norms of the "responsible disclosure" model in the security community. Social change would respond to the perception that "hackers" are inherently threatening by pressing researchers either to recapture that term's original meaning, or to abandon it. Finally, to ameliorate failures in the market for software vulnerability data, and to push such transactions into legitimate channels, we propose that a trusted third party act as a voluntary coordinator or clearinghouse for vulnerability deals.