When the government learns about a vulnerability in a piece of software or hardware, it can either stockpile that vulnerability for its own use or disclose it to the relevant software or hardware maker so that a fix can be implemented and distributed. The government thus faces a choice: Should it favor its offensive capabilities by keeping the vulnerability secret and potentially exploitable, or should it give the manufacturer the opportunity to fix its product?

The U.S. government's answer to that question, as reflected in rules released last week governing its disclosure of software vulnerabilities, is "it depends."

Initially developed by the Obama Administration, the so-called "Vulnerabilities Equities Process" (VEP) is an internal, executive-branch framework for determining when and whether the U.S. government should publicly disclose software and hardware flaws that it discovers that may leave computers vulnerable to attack. Once Obama's VEP was announced, experts debated the strategic value of the process, its effectiveness, the secrecy surrounding it (only a partially-classified version had been made publicly available), and how to reform it.

In particular, experts were concerned that the VEP did not adequately prioritize defense. By keeping software and hardware vulnerabilities secret from those who could fix them, individuals, businesses, and critical infrastructure that use the vulnerable technologies — and not only the government's targets — could be left open to attack.

The Trump administration clearly listened to these critiques, and the unclassified version of the "VEP Charter" issued this week is more comprehensive and transparent than its predecessor. In the debate over whether to favor offensive capabilities or defensive efforts, the document states that disclosure serves the national interest in the "vast majority" of cases.

To ensure that this conclusion isn't simply lip service, however, more reforms are needed. That's because the charter leaves some important questions unanswered and still fails to ensure that the decision-making is strongly weighed in favor of disclosure.

The Dangers of Stockpiling Vulnerabilities

As we have highlighted in several amicus briefs filed in cases challenging law enforcement hacking, government stockpiling of vulnerabilities creates security risks that experts do not know how to mitigate.

These include the risk that an attacker will steal and use malicious code for its own nefarious purposes, endangering businesses and human lives. For example, in 2016, the public learned that an entity calling itself the "Shadow Brokers" obtained National Security Agency malware. Following some initial attempts to sell the exploits, the Shadow Brokers dumped dozens of NSA hacking tools online for free in April 2017. One of those tools exploited a flaw in Microsoft software. Once it was released, others on the internet repurposed it into a virulent piece of ransomware that infected hundreds of thousands of computer systems worldwide in May 2017. The very next month, another malware attack combined that tool with another NSA exploit released by the Shadow Brokers. After initially hitting critical infrastructure in Ukraine, that attack spread internationally and infected hospitals, power companies, shipping companies, and the banking industry, endangering human life as well as economic activity.

Given these and other risks, the VEP process must be designed to carefully figure out when offense should take precedence over defense.

A New and Improved VEP?

The new VEP establishes a process for identifying the small minority of cases where law enforcement or intelligence interests override the benefits of disclosure, and it provides a list of considerations that officials should weigh in deciding whether to disclose. Laudably, these considerations reach beyond law enforcement and national security interests to include information security and other personal and commercial concerns. The VEP also establishes that any decision not to disclose a vulnerability is to be reviewed at least annually. There's also a process for a government agency to appeal a decision it doesn't agree with.

For the charter to be truly effective, however, it has to be designed so that intelligence and law enforcement interests won't be routinely favored over information security, commercial interests, innovation, and civil liberties.

That's where it gets complicated. One problem is that not every vulnerability the government uses will go through the VEP process. Only the vulnerabilities the government itself discovers are subject to the VEP. This means attack tools obtained from private vendors, who usually insist on non-disclosure agreements, are not subject to the VEP. Nor are tools that friendly governments let the U.S. use included. So, the VEP will only apply to a subset of vulnerabilities

The second problem is that the VEP's design is inclined to produce answers that favor offense. That's true for two reasons. First, the questions the VEP sets out for deliberation are mostly unanswerable. For example: What is the potential value of the government using a particular vulnerability? What are potential consequences? Can exploitation of this vulnerability by threat actors — like private hackers and foreign governments — be detected by the U.S. government or other members of the defensive community? How likely is it that threat actors will discover or acquire knowledge of this vulnerability if the government doesn't disclose it? Answering any one of these questions will require substantial guesswork.

Second, the people appointed to consider these unanswerable questions are disproportionately charged with an intelligence and law enforcement mission, and likely to favor those considerations over others.

The members of the "Equities Review Board" that have a civilian mission — the Department of State and Department of Commerce — are vastly outnumbered by those agencies with a military, intelligence, or law enforcement mission, such as the Office of the Director of National Intelligence, the Department of Homeland Security, the Department of Justice, and more. If no consensus is reached, a vote takes place. And if there's a vote, law enforcement and national security interests have a lot more votes. These interests may very well regularly win out.

That's because the officials in the room guessing the answers to the VEP questions will be strongly influenced by what they're getting graded on. If your job is to protect the public from terrorists or to spy on other nations, you're more likely to conclude that a vulnerability should be kept and exploited to help you accomplish your job. But if your job is to protect the public from ongoing data breaches, you're more likely to believe that the vulnerability should be disclosed to the vendor and patched before another hacker steals everyone's credit cards, personnel records, or online dating profiles.

Who should be in the room?

For one, the Federal Communications Commission should participate in these decisions, given how many of these exploits involve mobile communications technology. The same goes for the Federal Trade Commission, the agency most clearly charged with ensuring the public's privacy and data security.

The security risks from decisions about vulnerability disclosure are not theoretical. What's at stake is the security of the public and the internet at large. That's why we need a transparent, auditable VEP that values civilian interests and strongly favors disclosure. The Trump administration's updated process is one step in the right direction, but more reforms are needed. - **ACLU**


BCAP
Broadband
Cable Association
of Pennsylvania
127 State Street Harrisburg, PA 17101
717-214-2000 (f) 717-214-2020
bcapa.com
First in Broadband.
The Future of Broadband.®