White House Reveals How and When the US Keeps Security Flaws Secret

Dell Cameron
48 minutes ago •

Aerial photograph of the National Security Agency. (Photo: Trevor Paglen)

The White House on Wednesday revealed a 14-page document outlining the process the US government uses to determine how and when it tells private companies about security flaws; or conversely, under what circumstances it refrains from doing so.

It is known as the Vulnerabilities Equities Process (VEP). The purpose of the process, established under the Obama administration, is to review security bugs that software vendors aren't aware of—so called "zero-day" exploits. Since the vendor is unaware of the bug and a fix hasn't been deployed, zero days are highly sought after by criminal hackers, as well as those secretly sponsored by governments.

Since its inception, the VEP has been entirely opaque, even as the US intelligence community has been widely criticized for withholding details about critical exploits that have been used against businesses and consumers.

In the wake of the WannaCry attack this spring—made possible thanks to exploits stolen from the National Security Agency—Microsoft chief counsel Brad Smith openly criticized the US intelligence community for "stockpiling" vulnerabilities. "We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits," he said.

It appears the White House has heeded Smith's call and, facing industry-wide pressure, has made public a brief outline explaining how the government makes these determinations.

When a zero-day is discovered, it's submitted to a review board consisting of roughly a dozen executive departments and agencies, including the NSA, the Federal Bureau of Investigation, the Central Intelligence Agency, Homeland Security, and more. The NSA's representative is listed as the "executive secretariat" of the group, which is led by the White House cybersecurity coordinator, currently Rob Joyce.

After a vulnerability is submitted to the group, the agency representatives who make up what's called the Equities Review Board enter a five-day deliberation period in which they discuss whether or not to "discriminate" or "restrict" the vulnerability. If cyberattacks are ongoing involving the vulnerability being assessed, the process may be sped up considerably.

In determining whether to withhold knowledge about a security bug from the public, the review board considers a wide range of questions, according to the charter, from how likely threat actors are to exploit the flaw to what level of access a hacker must possess for it to work.

Other questions include:

> · Is exploitation of this vulnerability alone sufficient to cause harm?
>
> · What is the likelihood that adversaries will reverse engineer a patch, discover the vulnerability and use it against unpatched systems?
>
> · Will enough USG information systems, U.S. businesses and/or consumers actually install the patch to offset the harm to security caused by educating attackers about the vulnerability?
>
> · Can the product be configured to mitigate this vulnerability? Do other mechanisms exist to mitigate the risks from this vulnerability?
>
> · If a patch or update is released, how likely is it to be applied to vulnerable systems? How soon? What percentage of vulnerable systems will remain forever unpatched or unpatched for more than a year after the patch is released?
>
> · Can exploitation of this vulnerability by threat actors be detected by USG or other members of the defensive community?

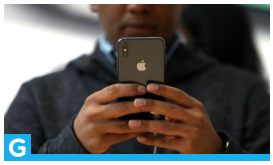
"Decisions whether to disclose or restrict a vulnerability will be made quickly, in full consultation with all concerned agencies, and in the overall best interest of USG missions of cybersecurity, intelligence, counterintelligence, law enforcement, military operations, and critical infrastructure protection," the charter says.

At an event in Washington DC early Wednesday morning, Joyce said that 90 percent of vulnerabilities are ultimately disclosed. It is the other 10 percent — presumably the most serious flaws, which the government intends to weaponize — that has security experts concerned.

Heather West, senior policy manager at Mozilla, praised the White House's decision to publish the charter, calling it a "critical step to help foster trust" between the government and tech industry. "We are pleased that the NSC recognizes the VEP is in dire need of more transparency and oversight, and we believe today's announcement makes significant progress towards these objectives," she said.

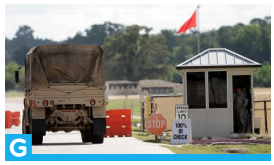
You can read the full VEP charter document below:

RECOMMENDED STORIES



How Black Market Criminals Are Duping Apple Users Into Surrendering Their iPhones

Julian Assange's Secret DMs to Donald Trump Jr. Are Somehow Dumber, Sadder Than You'd Think



Texas Paid Hundreds of Thousands to Spy on Cellphones With Surveillance Planes

ABOUT THE AUTHOR

Dell Cameron

Dell Cameron

Dell Cameron is a staff reporter at Gizmodo.

Email Twitter Posts Keys