The Vulnerabilities Equities Process

What we know and what we'd like to see

The Vulnerabilities Equities Process (VEP) is the U.S. Government's process for reviewing vulnerabilities that it learns about in order to decide whether to share those vulnerabilities with affected companies (allowing the companies to patch these vulnerabilities) or withhold them for operational purposes. These operational purposes include law enforcement investigations, intelligence collection, and "offensive" exploitation. The government learns about these vulnerabilities through its own research and development, by purchasing them, through intelligence work, or by reports from third parties.

Disclosing these vulnerabilities to affected companies allows companies to: patch them quickly; increase the security, privacy, and safety of their systems and users; reduce conflict and improve trust between companies and government; and, especially for organizations with limited cybersecurity resources, benefit from external discovery of vulnerabilities in their products and systems that they may not otherwise have the resources to find.

The origins of the VEP can be traced to the National Security Policy Directive 54, signed by President George W. Bush in 2008. The process was finalized in a document dated February 2010, but was not broadly or consistently implemented until April 2014 following the revelations of the Heartbleed vulnerability which is estimated to have affected two thirds of the world's web servers. At that time, the White House Cybersecurity Coordinator Michael Daniel announced in a blog post that the he had "reinvigorated" the VEP.

The VEP has continued to meet and is operational under the Trump Administration, but reports are that it is handling a smaller volume of vulnerabilities (we don't know why). As far as we know, the VEP operates much in the same way and with the same policies under President Trump as it did under President Obama, but with such an opaque process, it's hard to say that with certainty.

While the process itself is largely shrouded in secrecy, a few key procedural and transparency reforms, the VEP can be a strong mechanism for ensuring the government is handling vulnerabilities responsibly.

The VEP should be required by law, with clear process and review requirements

There is no legal obligation on the government to share the vulnerabilities that it learns about with affected companies, and putting the vulnerability or exploit through the VEP is entirely voluntary. As such, there is no requirement that an agency submit a vulnerability for review by the VEP, and indeed former FBI Director Comey has stated that the FBI chooses not to in many cases. Additionally, the agency can choose when to "nominate" the vulnerability to the VEP, without limit on how long it is held or exploited before they do so. And once the vulnerability does enter the VEP, there is not a public description of how the process operates or what considerations are a part of the deliberations.

Reforms: We want all vulnerabilities that the government learns about to go through a robust, accountable, and transparent process to ensure all interests and risks are considered, and that all vulnerabilities are eventually disclosed to the affected companies. To accomplish that, the VEP, or a process like it, should be established in law in order to ensure that it continues to do this important work. This should also codify both the presumption that vulnerabilities will be disclosed promptly to the relevant companies and a robust, accountable, and transparent process for reviewing delays in disclosure. Codifying the VEP into law would protect it and ensure the process is followed no matter who is in power.

We look forward to working with policymakers to implement these key reforms to the VEP.

For further information, please contact: Heather West, Senior Policy Manager | heather@mozilla.com

The VEP should include civilian consumer security and protection agencies
In the past, the VEP has sometimes been dominated by intelligence community or law enforcement voices urging operational use of an exploit without balancing voices from agencies with consumer security and protection missions. VEP participants sometimes use an exploit's classification level to exclude participants from civilian agencies that would be primarily motivated by maintaining ecosystem and user security.

Reforms: All relevant agencies should be involved in the VEP to ensure a broad set of risks and interests are considered. In particular, the Departments of Homeland Security and Commerce should be core participants in the VEP. Other agencies such as the Department of State, the National Economic Council, the Federal Trade Commission, the Department of Energy, and other agencies should be involved in the VEP when there is a vulnerability that is relevant to them. Other agencies with relevant expertise to a particular vulnerability -- such as in cars, medical devices, and other Internet of Things devices -- should also be involved as needed.

The VEP should have transparency and oversight
There is currently no regular reporting to Congress or the public about VEP determinations, or on the instances where the VEP's policies and practices were not adhered to. There seems to be no independent oversight at all.

Reforms: Regular reporting to Congress and the public about VEP determinations as well as on any instances where these policies and practices were not adhered to. VEP processes should also be reviewed by relevant Inspectors General and the Privacy and Civil Liberties Oversight Board.

The VEP should be administered by DHS
While the VEP officially lives within the White House National Security Council, it is still administered by the NSA. While the NSA has some staff dedicated to the VEP, the VEP is largely staffed by individual agencies who assign staff to particular negotiations. Once a decision to disclose is made, there is not a standard process by which the vulnerability is disclosed, despite significant expertise existing within the Federal government on best practices around vulnerability disclosure via the National Cybersecurity Communications and Integration Center (NCCIC) and US-CERT and ICS-CERT.

Reforms: The Executive Secretariat of the VEP should be housed in the Department of Homeland Security while continuing to live institutionally within the NSC in order to enable interagency deliberations, information sharing, and disclosure processes. In this role, DHS should have dedicated staff to assist in the assessment of vulnerabilities with primary responsibility to coordinate disclosure of vulnerabilities.

The VEP should disclose according to best practices
While there are well-understood mechanisms and existing coordinated vulnerability disclosure programs within the government and industry, the VEP does not usually utilize them. Instead, the agency which nominated a vulnerability to the VEP may handle the disclosure, even if they lack the expertise, infrastructure, and trust in the community to do so. Indeed, there are now multiple examples of exploits from various U.S. entities being released - and quickly weaponized against users of major technology products.

Reforms: By placing the VEP at DHS, it can utilize the US-CERT and ICS-CERT disclosure infrastructure within the DHS National Cybersecurity and Communications Integration Center (NCCIC) which has built up the requisite expertise, infrastructure, and trust in the community to do so.

We look forward to working with policymakers to implement these key reforms to the VEP.
For further information, please contact: Heather West, Senior Policy Manager | heather@mozilla.com