The Vulnerabilities Equities Process

A brief history

The Vulnerabilities Equities Process -- most commonly referred to by its acronym VEP -- is the US Government's process for reviewing vulnerabilities that it learns about and deciding whether the vulnerabilities should be shared with the affected companies. The government learns about these vulnerabilities through its own research and development, by purchasing them, through intelligence work, or by reports from third parties. The VEP brings together some - but not all - of the interagency stakeholders for this decision making. The VEP is not codified in law or executive order, as such there is no current legal requirement for Federal agencies to submit vulnerabilities that they learn about to the VEP.

A vulnerability is a technical design or implementation flaw in an information technology product or system that can be used to exploit or penetrate a product or system. These vulnerabilities can put users and businesses at significant risk from bad actors. At the same time, exploiting these same vulnerabilities can also be useful for law enforcement and intelligence operations.

The VEP remains shrouded in secrecy, and is in need of process reforms to ensure appropriate transparency, accountability, and oversight.

- *January 2008* - President George W. Bush signed the National Security Policy Directive 54 (NSPD 54), which called for a US-government-wide effort called the Comprehensive National Cybersecurity Initiative (CNCI). CNCI required the Departments of State, Defense, Homeland Security, and Justice, as well as the Director of National Intelligence, to develop "a joint plan for the coordination and application of offensive capabilities to defend US information systems."
- *2008* - The joint plan coming out of the CNCI notes that the discovery of vulnerabilities "may present competing equities for [government] offensive and defensive mission interests" and recommended that "actions taken in response to knowledge of a specific vulnerability must be coordinated to ensure the needs of each of these 'equities' are addressed." The joint plan recommended the development of a "Vulnerabilities Equities Process," but the tasks assigned to the VEP in the joint plan remain classified.
- *2008-2009* - Starting in 2008, in accordance with the joint plan's recommendation, the Office of the Director of National Intelligence (ODNI) set up a working group to develop the VEP. The working group included representatives from ODNI, the National Security Council, Central Intelligence Agency, Defense Intelligence Agency, Justice Department, Federal Bureau of Investigation, Department of Defense, Department of State, Department of Energy, and Department of Homeland Security. The working group developed a document known as the "Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Equities Policy and Process" (the VEP Document). The VEP Document is dated February 16, 2010.
- *April 11, 2014* - Bloomberg published an article claiming that the NSA had, for two years, been exploiting a vulnerability called Heartbleed which is estimated to have affected two thirds of the world's web servers - any server that used the popular OpenSSL cryptographic library.

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

- *April 28, 2014* - White House Cybersecurity Coordinator Michael Daniel published a blog post denying that the government had prior knowledge of Heartbleed and discussing how he is "reinvigorating" the VEP. It is widely believed that the VEP was not operational at this time. Before the VEP was operationalized, it appears that various Federal agencies ran their own processes -- notably, the NSA had long run a process to navigate the potentially conflicting missions of its Information Assurance and Signals Intelligence Directorates.
- *May 6, 2014* - EFF filed a Freedom of Information Act (FOIA) request to get all records pertaining to the VEP.
- *December 15, 2014* - EFF received first (heavily redacted) batch of responsive documents, continued to get additional documents over the next year.
- *January 14, 2016* - EFF received a largely unredacted description of the VEP including the VEP Document following litigation to compel response to their May 6, 2015 FOIA.
- *March 2016* - The FBI contracted with a security firm to break into an iPhone used by the San Bernardino shooter, in the midst of a high profile lawsuit to force Apple to write software to unlock the security features on the phone.
- *April 27 2016* - The FBI released a statement saying the Bureau will not submit the iOS vulnerability in question for review by the VEP, saying it did not possess enough information about how it worked.

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